Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Programa Especial de Titulación:

"Diseño e Implementación del Centro de Operaciones de Seguridad para el Evento Deportivo Juegos Panamericanos Lima 2019"

Autor: Acero Bendezú Jheancarlo

para optar el Título Profesional de

Ingeniero de Telecomunicaciones

Lima – Perú

2020

Índice

CAPÍTULO III

DESARROLLO DE LA SOLUCIÓN

CAPÍTULO IV

RESULTADOS

INDICE DE TABLAS

INDICE DE FIGURAS

Resumen

En el presente proyecto se presenta el diseño la implementación de un Centro de Comando de Seguridad (COS) para el evento deportivo Juegos Panamericanos Lima 2019, el cual tiene el propósito de reducir la inseguridad dentro y fuera de los recintos deportivos, salvaguardando la seguridad de los asistentes al evento deportivo. El uso de tecnología es esencial para la seguridad a través de video vigilancia en la siguiente solución presentada los operadores podrán administrar todas las cámaras de manera remota usando una plataforma globalizada que integra varias plataformas de videos independientes. Este proyecto realizara un análisis cuantitativo sobre la reducción de incidentes durante el proceso de los juegos panamericanos Lima 2019.

Introducción

El centro de operaciones de seguridad (COS), es un centro que pertenece a una organización con funciones exclusivas en temas de seguridad, ejecuta trabajos de monitorio de video vigilancia por medio de soluciones tecnológicas orientadas a la seguridad y con operadores especializados que monitorean todos los acontecimientos en tiempo real. El COS brinda servicios de seguridad de acuerdo con las normas y objetivos de la organización, significa que los servicios que puede brindar varían dependido a la organización.

Los eventos deportivos de gran magnitud como es el caso de los Juegos Panamericanos Lima 2019, donde se concentran mayor cantidad de individuos son lugares susceptibles a las causas que generan la inseguridad por lo tanto se debe tener mayor control del entorno ya sea externo o interno, la implementación de tecnología es esencial para el control y monitoreo, para poder prevenir y actuar en distintos casos de inseguridad.

En este proyecto se desarrollará el Diseño e implementación un Centro de Operaciones de Seguridad para el evento deportivo Juegos Panamericanos Lima 2019 y el análisis de la reducción de incidencias que se generan durante el progreso del evento deportivo.

A continuación, se describe un resumen de los capítulos del proyecto.

Capítulo 1, se presenta la problemática del tema a tratar, justificación, objetivo principal y secundarios, alcances y limitaciones, justificación y estudio de viabilidad.

Capítulo 2, se expone antecedentes nacionales e internaciones y el marco teórico utilizado para la realización del proyecto.

Capítulo 3, se describe el proceso de desarrollo del proyecto y el análisis de incidencias.

Capítulo 4, se presenta los resultados de la realización del proyecto y del análisis de incidencias.

CAPÍTULO I
ASPECTOS GENERALES

1.1. Definición del Problema

1.1.1. Descripción del Problema

En todo en el mundo existe la inseguridad ciudadana, victimización, delitos, violencia entre otros son palabras que se asocian a la inseguridad, problema principal que aumenta si no es controlado y mitigado. El incremento de inseguridad genera malestar en la población física y psicológicamente. Los eventos de gran magnitud donde se concentran mayor cantidad de individuos son lugares susceptibles a las causas que generan la inseguridad por lo tanto se debe tener mayor control del entorno ya sea externo o interno, la implementación de tecnología es esencial para el control y monitoreo, para poder prevenir distintos casos de inseguridad (Lio, 2015).

Los juegos panamericanos 2007 se realizaron en la ciudad de Rio de Janeiro, el evento deportivo se realizó en un ambiente pacífico y seguro, creando un sistema nuevo de seguridad nacional, iniciando un modelo nacional de seguridad publica juntamente con la ciudadanía. El proyecto fue desarrollado para poder mejorar la seguridad de los asistentes en el evento deportivo y mitigar los incidentes que atenten contra la seguridad, en este proyecto se unieron el ejército nacional, la fuerza policial y la comunidad

(programas sociales). El proyecto fue liderado por la secretaria nacional de seguridad pública (Ministerio do Esporte, 2013).

Según la Consultora Mercel (2018). La ciudad de Lima se ubica en el puesto 8 de las 11 ciudades de Sudamérica menos segura. Esto quiere decir que tenemos una brecha de seguridad el cual tenemos que dar solución si se desea ser anfitrión de uno de los eventos deportivos más importantes del continente, la aglomeración de personas sin la supervisión o control genera más inseguridad y pone en riesgo a los participantes de ser víctima de actos que atenten contra la seguridad.

En este sentido durante los Juegos panamericanos Lima 2019, el Estado tiene la obligación de salvaguardar y cuidar por la seguridad de todos los asistentes nacionales y extranjeros que visitaran la ciudad durante la disputa deportiva. Es necesario asegurar un entorno seguro y pacifico mediante la unión de la policía nacional del Perú, el ejército nacional, el serenazgo municipal, empresas privadas (asociación) y la comunidad (voluntariado). Se requiere instalar una infraestructura tecnológica necesaria como también sistemas de inteligencia para la planificación y coordinación de evaluaciones de peligro y precaución de las posiciones que puedan conjeturar una amenaza para el éxito o desarrollo de los juegos (Regalado, Ayala, Chero, Yauri, & Zevallos, 2015).

1.2. Definición de Objetivos

1.2.1. Objetivo general

Diseñar e implementar un Centro de Operaciones de Seguridad para el evento deportivo Juegos Panamericanos Lima 2019.

1.2.2. Objetivos específicos

- Qué relación tiene diseñar e implementar los módulos de monitoreo al Centro de operaciones de Seguridad para administrar y monitorear

remotamente las plataformas de video independientes de las sedes deportivas en el evento deportivo de los Juegos Panamericanos Lima 2019.

- Qué relación tiene diseñar e implementar un sistema que integra todas las plataformas de Video independientes en el Centro de Operaciones de Seguridad de las sedes deportivas del evento deportivo de los Juegos Panamericanos Lima 2019.
- Que relación tiene diseñar e implementar de reducción de incidentes en el diseño e implementación de un Centro de Operaciones de Seguridad durante el evento deportivo juegos panamericanos lima 2019.

1.3. Alcances y limitaciones

1.3.1. Alcances

Dar acceso a los operadores de administrar y visualizar las trasmisiones en vivo provenientes de los equipos de video vigilancia, reproducir grabaciones de la plataforma de video de las diferentes sedes deportivas de los juegos panamericanos. Visualizar el origen del video de varias cámaras simultáneamente, mediante distintas opciones de distribución de pantalla. El centro de operaciones de seguridad debe soportar distintos tipos de Video Manager software, cámaras y equipos de video. Se diseñará un sistema de almacenamiento de video con la capacidad de retener la grabación en un periodo de 7 días, registrar 761 cámaras de las sedes deportivas y dispositivos móviles.

1.3.2. Limitaciones

Realizar las acciones técnicas en cada solución que permitan el correcto funcionamiento del centro de operaciones de seguridad (COS). Mediante la instalación y el mantenimiento preventivo, correctivo o rehabilitación, con la finalidad de que los sistemas sean optimizados y tengan una menor probabilidad a fallas. El COS tiene 27 estaciones de trabajo, las cuales se

distribuirán para el monitoreo de la Seguridad Ciudadana y para la Seguridad Deportiva.

No se consideran los equipos de la solución de Radio Troncalizados, ni activos que sean de responsabilidad del edificio (LCC).

1.4. Justificación

La LI Asamblea General de la Organización Deportiva Panamericana - ODEPA, eligió al Perú como anfitrión de los XVIII Juegos Panamericanos del 2019; mediante Resolución Suprema Nro. 006-2015-MINEDU modificado por Resolución Suprema 003-2017-MTC se publicó de interés nacional los XVIII Juegos Panamericanos 2019 y se creó una comisión organizadora con el objetivo de preparación, coordinación y realización de los trabajos enlazados con los XVIII Juegos Panamericanos del 2019. El comité organizador, en adelante COPAL, aprobó un proyecto de diligencia que incluyó el proyecto Maestro de Operaciones, Infraestructura y Gestión como modelo para el desarrollo de los Juegos Lima 2019. Dicho Plan Maestro General de los Juegos fue expuesto y a la Organización Deportiva Panamericana (ODEPA) el mismo que guía la gestión del Proyecto Especial. Por Decreto Legislativo Nro. 1335 se transfiere al Ministerio de Transportes y Comunicaciones el Proyecto Especial y con fecha 11 de octubre de 2017 mediante la Resolución Ministerial Nro. 1000-2017-MTC/01 se aprobó el Manual de Operaciones del Proyecto Especial, cuyo artículo 31° señala que la Gerencia de Operaciones es la institución responsable de la gestión de las acciones y actividades relacionadas, entre otros, con los deportes, sedes deportivas, alojamiento, relaciones internacionales, transporte, seguridad, servicios médicos, alimentación, limpieza y manejo de residuos sólidos para el desarrollo de los Juegos. Los eventos deportivos, contribuyen al crecimiento del deporte aficionado y profesional del Perú, fomentando su ensayo, activando el crecimiento económico y social de una nación, a través de la promoción del turismo, la generación de oportunidades de trabajo y divisas, entre otros aspectos. En ese sentido, los bienes a adquirir tienen la finalidad de atender los requerimientos

de la Gerencia de Operaciones en el marco de sus funciones, para cumplir con los estándares que la organización exige, atendiendo oportunamente las actividades operativas que contribuirán al éxito durante el crecimiento de los XVIII Juegos Panamericanos del 2019 declarado de interés nacional.

1.5. Estudios de viabilidad

El siguiente proyecto fue aprobado por el comité organizador panamericanos Lima 2019, en convenio celebrado entre el ministerio de trasporte y comunicaciones y la oficina de naciones unidad para proyectos. El cual financiara la ejecución del proyecto de inicio a fin, donde se utilizarán los recursos tecnológicos y la infraestructura existente del Centro de Comando, Control y Comunicaciones (C4), tales como (equipos, soluciones, softwares, etc.). Actualmente, las soluciones tecnología a implementar en el nuevo centro de operaciones de seguridad es de fácil acceso en el mercado nacional o también en el mercado internacional. El tiempo de duración del desarrollo del proyecto es de 6 meses y como fecha final es el inicio de los Juegos Panamericanos Lima 2019.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes

2.1.1. A nivel Internacional

Lahoz (2017) Diseño de Redes de Cámaras Inteligentes Utilizando Smartphones. (tesis de pregrado). Indica que: Usan una herramienta de software para el control de forma remota de una red de cámaras inteligentes utilizando smartphones Android, el análisis muestra que la red de cámaras podrá estar compuesta por varias cámaras coordinadas por un mismo servidor. Las cámaras graban la imagen y proceden a realizar la conversión al formato JPEG y envían al servidor, el servidor se encarga de hacer de intermediario entre las cámaras y la aplicación del cliente. La video vigilancia en tiempo real es la función principal de este diseño compuesto de smartphones.

Lahoz (2017) Concluye que la trasmisión de video de una calidad alta genera cuello de botella, ya que los propios celulares no tienen la capacidad para procesar y trasformar las imágenes por segundo.

Martí (2013) Diseño de un Sistema de Televigilancia sobre IP para el Edificio CRAI de la Escuela Politécnica superior de Gandia. (tesis de pregrado). Indica que: El edificio CRAI tiene 2 pisos y un sótano parcialmente abierto, existe una preinstalación de cableado de red tanto cable UTP como

cableado de fibra óptica, se ha optado una solución de CCTV sobre IP siendo mínimo los costes de instalación de red, un análisis indica que será necesario 34 cámaras distribuidas estratégicamente en el interior y exterior del edificio. La capacidad de almacenamiento de la información está diseñada para albergar hasta 30 días, en el centro de control se instalará la plataforma de video IVMS-4000 V.2 que permitirá administrar y operar toda la instalación CCTV.

Martí (2013) Concluye que se debe tener personal capacitado para la administración del centro de control del edificio CRAI, el sistema CCTV fue desarrollado pensando en la escalabilidad a futuro y el diseño del proyecto fue enfocado para la reducción de la inseguridad.

Buendía, (2016) Diseño e Implementación de un Sistema Completo de Seguridad que Contempla Video Vigilancia Móvil y posicionamiento Global GPS en Tiempo Real, con Monitoreo Remoto para Vehículos Blindados de Transporte de Valores. (tesis de pregrado). Indica que: El proyecto permita visualizar en tiempo real a través del uso de cámaras móviles y permita determinar la ubicación exacta cada 5 minutos. La tecnología a emplearse será a través de tecnología de comunicación de tercera generación (3G) no se usará las redes (4G) por su cobertura limitada en ecuador, el sistema integra tecnología (3G) para la comunicación permanente al centro de monitoreo, con tecnología WI-FI para gestionar la comunicación interna de manera inalámbrica para el respaldo de archivos de audio y video, y tecnología GPS para el monitoreo de las ubicaciones exactas del vehículo blindado. Procede con la instalación de cámaras internas y externas del vehículo con juntamente con la instalación de los micrófonos, el sistema estará conectado a un grabador móvil (MVDR) que cuenta con la tecnología de requerida para la comunicación con las redes (3G), redes WI-FI y GPS. El sistema móvil se completa con la instalación del programa de administración de video en un servidor, el sistema estará conectado a un centro de control que podrá ser monitoreado en tiempo real, podrá controlar las cámaras y permitir la localización del GPS.

Buendía, (2016) Concluye que el sistema de seguridad móvil se encuentra recién en desarrollo y hay muy pocas soluciones para este tipo de problemas en ecuador, el gobierno debe indicar que los vehículos blindados deben contar con este tipo de sistemas de seguridad y el sistema propuesto no es completamente adaptable al escenario móvil, pero con las pruebas realizadas se concluye la satisfacción del cliente.

2.1.2. A nivel Nacional

Salcedo, C. (2018). Diseño de un Centro de Control y Monitoreo (CCTV) con Sistema de Radio Enlace para la Seguridad en la Municipalidad de Islay Matarani, Arequipa 2018. (tesis de pregrado). Menciona lo siguiente: La investigación tiene como objetivo proponer un diseño de un centro de control y monitoreo para que mitigue la delincuencia en la ciudad de Islay Matarani, realiza un estudio para identificar las zonas y los agrupa en niveles. Salcedo diseña la ubicación y el número de las cámaras que salvaguarde la seguridad, su centro de control se diseña para dos operadores y un supervisor, conjuntamente implementa un software que cuenta con todas las herramientas para monitoreo y vigilancia. Además, propone utilizar un sistema de radio enlace para la comunicación de las cámaras por los factores geográfico y económico.

Salcedo, C. (2018) indican en sus conclusiones que el sistema tiene la capacidad de almacenar información hasta 30 días, su centro de control garantiza el monitoreo constante de todas las zonas y el cumplimiento con las normas de la actual legislación peruana para su correcto funcionamiento.

Salcedo, C. (2018) Recomienda que la municipalidad debe realizar un estudio de los pozos a tierra previo a la instalación, los operadores a cargo del centro de control y monitoreo deben estar capacitados en el uso de la plataforma de video vigilancia.

Camacho, E. (2017). Análisis y Diseño de un Sistema de Video Vigilancia (CCTV) con Fibra Óptica Aplicando la Norma IEEE 802.3bm para

el Club Internacional Arequipa. (tesis de pregrado). Indica que: El estudio de un sistema de video vigilancia en el club internacional de Arequipa, donde recogió de información del personal del club con el fin de detectar e identificar los tipos de delitos cometidos dentro y fuera de los alrededores del club. El estudio debe prevenir y salvaguardar la integridad de los trabajadores, socios y personas que visiten las instalaciones del club, en su análisis determina el número de cámaras a utilizar, su centro de control cuenta con cuatro operadores y un supervisor. Camacho utiliza un software que cuenta con las herramientas necesarias para la administración de video vigilancia, el centro de control cuenta con un data center como nodo central e interconecta todas cámaras a través de fibra óptica para garantizar el ancho de banda y la calidad de las imágenes.

Camacho, E. (2017) Concluye que el estudio se realizó después de identificar las zonas de riego para garantizar la vigilancia las 24 horas del día, el análisis del sistema determina que puede almacenar 30 días de grabación y se cumplió con los parámetros de la norma IEEE 802.3bm.

Camacho, E. (2017) Recomienda realizar estudios de los sistemas previo a la instalación, la ubicación de las cámaras debe estar en lugares estratégicos y el personal a cargo debe estar capacitado en el manejo del software de monitoreo.

Sierra (2017). Propuesta del Sistema de Video Vigilancia en la Seguridad Ciudadana Distrito de Pueblo Libre 2016-2020. (tesis de posgrado). Menciona lo siguiente: La investigación tiene como objetivo implementar y articular el sistema de video vigilancia para mitigar el problema de la inseguridad ciudadana en el distrito de Pueblo Libre, el estudio recoge información y determinar puntos críticos. El análisis se realizó en lugares donde se requiere cámaras y centros de control para su descentralización, se determinó que se debe aumentar 60 cámaras y 6 centros de control, habiendo realizado comparaciones con otros gobiernos locales, la comunicación y articulación de la Municipalidad de Pueblo Libre con la Policía Nacional, Serenazgo y los

Comités de las Juntas Vecinales es eficaz y eficiente para contrarrestar actos delictivos en el distrito.

Sierra (2017) El resultado de los análisis reveló que del 2015 al 2016 se ha incrementado en un 31.8 %. Luego se procedió a presentar propuestas para el mejoramiento de video vigilancia en el distrito de Pueblo Libre, siendo el objetivo principal la prevención del delito. En el 2017 existen 77 cámaras en vigencia y operando con normalidad y aproximadamente 60 cámaras que presentan problemas con tendencia que seguirá hasta el 2020. Se determino la instalación 6 centros de control tomando en consideración los lugares de alto transito ciudadano y afrontar el problema de la inseguridad en conjunto con la Policía Nacional, Serenazgo y los Comités de las Juntas Vecinales.

Sierra (2017) Concluye que falta implementación de cámaras de vigilancia en el distrito de Pueblo Libre, falta de recursos financieros y falta de capacitación a los técnicos. Falta cubrir puntos críticos de incidencia delictiva, los instalados no son suficientes.

Sierra (2017) Recomienda más inversión en los sistemas de video vigilancia, implementar cámaras en puntos sensibles o áreas estratégicas.

2.2. Tecnologías/técnicas de sustento/definición de términos

2.2.1. Sistema de Centro y Control

Un sistema de centro y control, o comando y control está constituido por ambientes debidamente seleccionados, equipos, comunicaciones, procedimientos y por un personal que resulten vitales para el comandante pueda planificar, dirigir y controlar las operaciones de las fuerzas asignadas, a efectos del cumplimiento de las misiones correspondientes y dar respuestas inmediatas a las contingencias que se presentan (Pérez, 2009).

2.2.2. Modelo Teórico de comando y Control

El comando y control es como un bucle infinito, el modelo se inició en un principio para mejorar el accionar de los pilotos de cazas y su relación con la aviónica que descargaron en la definición del Bucle OODA (Observar, Orientar, Decidir y Actuar) por parte J. Boyd, expiloto de combate y destacado asesor militar del gobierno norte americano. Este acercamiento a realizado todo un modelo en el área de comando y control, en el que se muestra el entorno (Observar), se construye la visión de la escena de operaciones (Orientar), se toma las decisiones oportunas (Decidir) y por último se procede sobre el entorno (Actuar) (Pérez, 2009). En la Figura 1, se puede observar el diagrama del bucle OODA.

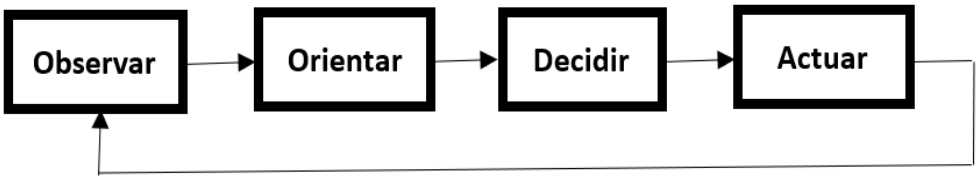


Figura 1. Bucle OODA simple

Fuente: Arquitectura de un sistema C4ISR para pequeñas unidades (Pérez, 2009)

2.2.3. Centro de Comando, Control, Computo y Comunicaciones

Los sistemas de comando y control evolucionaron convirtiéndose en centro de comando, control, cómputo y comunicaciones (C4). No solo fue un cambio de conceptos, siguió un proceso de evolución en las tecnologías disponibles en específico en el sector de las telecomunicaciones Instituto Militar de Estudios Superiores Escuela de Comando y Estado Mayor s. (2006) afirma. El sistema (C4) está desarrollado básicamente para las siguientes eventualidades de apoyo al comando y control:

- Adquirir una cantidad relevante de información de múltiples sistemas.
- Procesar la información recolectada y presentarla adecuadamente para apoyar la toma decisiones.

- Permitir la transmisión de órdenes a cualquier nivel a través de una importante red de telecomunicaciones.

El modelo (C4) se basa en dos pilares fundamentales:

- La digitalización de la información: Los recursos disponibles son optimizados en las vías de las telecomunicaciones. Cuando en el pasado se tenía a disposición solo un canal de voz, en la actualidad existe la posibilidad de varios canales, datos, video, usando al máximo los medios de comunicación físicos e inalámbricos.

- La interoperabilidad: Es un concepto importante entre otros para el crecimiento de un modelo de mando y control.

2.2.4. Centro de Operaciones de Seguridad

Morales, Moreno, y Ortigoza (2014) Afirma. El centro de operaciones de seguridad (COS), es un centro que pertenece a una organización con funciones exclusivas en temas de seguridad, ejecuta trabajos de monitorio de video vigilancia por medio de soluciones tecnológicas orientadas a la seguridad y con operadores especializados que monitorean constantemente en tiempo real a toda hora y todos los días de la semana. El COS brinda servicios de seguridad de acuerdo con las normas y objetivos de la organización, significa que los servicios que puede brindar varían dependido a la organización, pero existen funciones importantes que un centro de operaciones de seguridad debe tener como pilares fundamentales las cuales se muestran en la Figura 2.

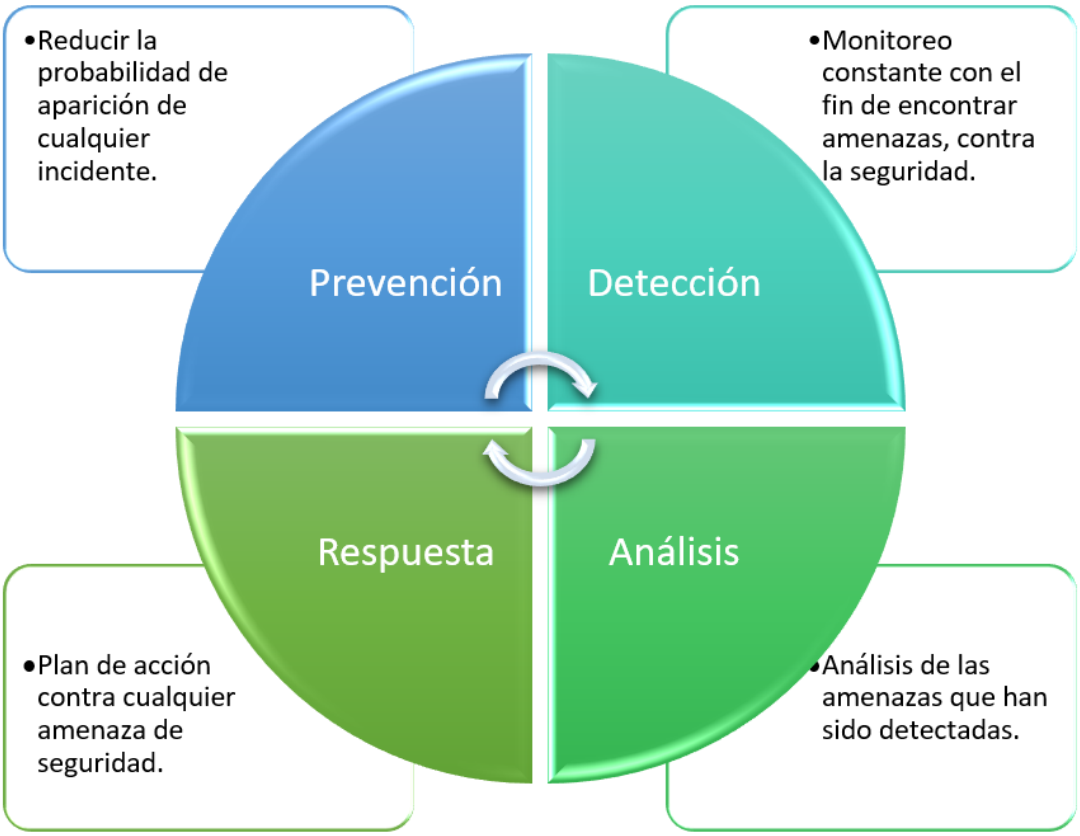


Figura 2. Pilares fundamentales del COS

Fuente: Propuesta de un modelo de centro de operaciones de seguridad (SOC) para fuerza aérea colombiana Morales, Moreno, y Ortigoza (2014).

2.2.5. Sistema de Gestión de Video

Axis Comunicactions Corp. (2018). Actualmente en el mercado se manejan varios sistemas de gestión de video que están desarrollados para los sistemas operativos existentes en el mercado como: Windows, Linux y Mac Os. Para el crecimiento de este modelo de gestión es necesario tener en consideración la plataforma de hardware, software, la administración de seguridad y la posibilidad de integración de equipos con diferente sistema operativo. En la Figura 3 observamos un ejemplo del software de gestión de video.

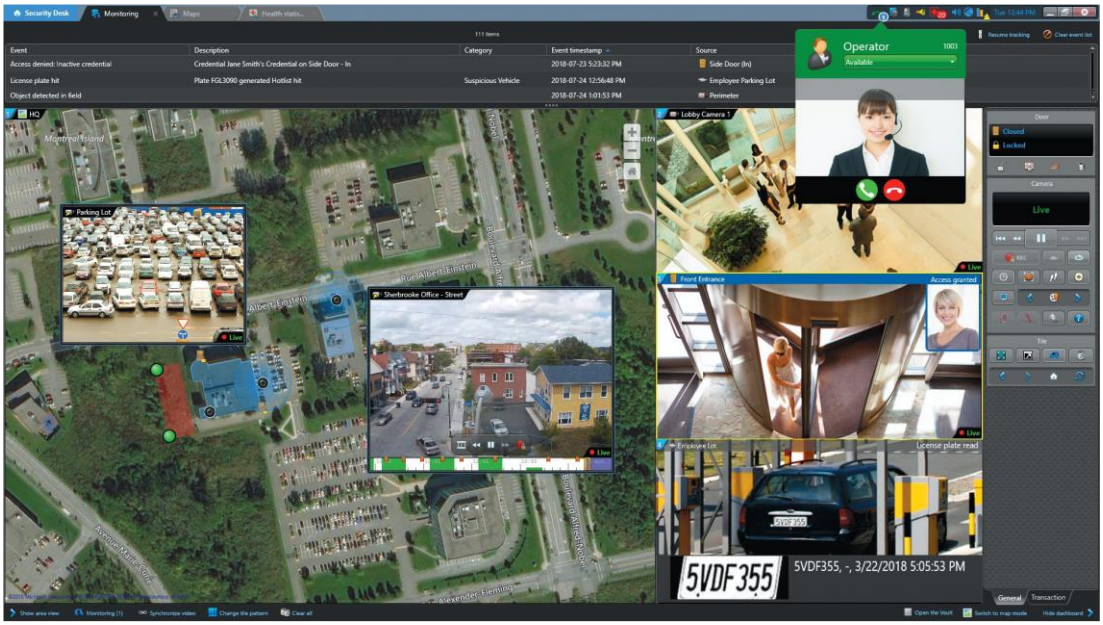


Figura 3. Software de gestión de video

Fuente: Genetec security center seguridad unificada integral (Genetec Inc. , 2018).

2.2.5.1. Plataforma de hardware

Un modelo de gestión de video en red tiene tipos de plataformas de hardware.

2.2.5.1.1. Plataforma de servidor

Axis Comunicactions Corp. (2018) Este producto de gestión de video está apoyado en la implementación de un sistema de servidores en la cual puede contener servidores para la plataforma de video como servidores de almacenamiento con el objetivo de tener un mejor rendimiento del sistema. Uno de los veneficios principales es que te da la completa libertad de aumentar el rendimiento según a tu necesidad puedes adquirir distintos productos que complementen y aumenten la potencia de la plataforma de video, también permite la integración de nuevos servicios ejemplo: control de alarmas, control de acceso, control industrial, etc. Estas posibilidades permiten a los operadores tener más control a través de un software cliente. En la Figura 4 podemos observar el ejemplo de un diseño basado en plataforma de servidor.

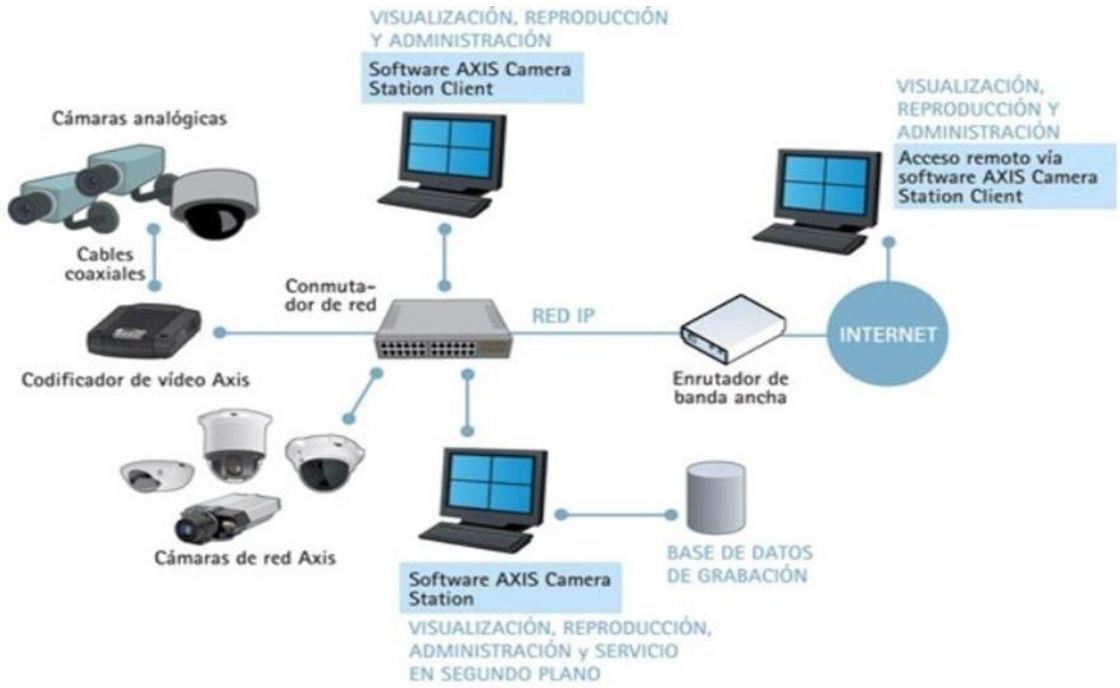


Figura 4. Sistema de video vigilancia en red basado en servidor.

Fuente: Sistemas de gestión de video Axis Comunicactions Corp. (2018).

2.2.5.1.2. Plataforma de video en red

Según Axis Comunicactions Corp. (2018) este producto de gestión de video basada en Network video Recorder (NVR), Es un ordenador con software preinstalado con funciones de gestión de video por lo general el software y hardware son patentados por su fabricante, tiene como dedicación realizar tareas específicamente de reproducción de video en red, análisis y grabación. Su sistema mayor mente está diseñada para que no pueda integrarse con nuevas funcionalidades y puede estar desarrollado en Windows, Linux o S.O. patentado. El objetivo del NVR es ofrecer un rendimiento óptimo para plataformas de video que contengan una menor densidad de cámaras y que estén dentro de sus límites, esta solución es menos escalable que la solución basada en servidor. En la Figura 5 podemos observar el ejemplo de un diseño basado en plataforma de grabador.

Figura 5. Un sistema de video vigilancia en red que utiliza un NVR

Fuente: Sistemas de gestión de video

2.2.5.2. Plataforma de Software

En el mercado existen múltiples plataformas de software con funciones distintas para la gestión de video, uno de los servicios principales que contienen estos sistemas es la interfaz web (Axis Comunicactions Corp., 2018)

2.2.6. Almacenamiento y ancho de banda

El almacenamiento y el ancho de banda de red son fundamentales en la estructura de un sistema de video vigilancia, que contienen variables a calcular. Entre las variables se encuentran: la comprensión (Motion JPEG, MPEG-4, H.264, etc.), la resolución de imágenes, el número de cámaras, frecuencias de imágenes, grabación escenarios o continua, horas de grabación y complejidad de escenas (Axis Comunicactions Corp., 2018).

2.2.6.1. Red de almacenamiento por área

Storage área network (SAN) o en español red de almacenamiento por área, son redes dedicados a la alta velocidad para almacenamientos en áreas, conectadas principalmente por fibra a uno o varios servidores. Las SAN se desarrollaron con el fin de acrecentar la productividad de las aplicaciones y mejorar la disponibilidad al disminuir la alta demanda de datos de almacenamiento de la LAN, la fibra se

suele usar para ofrecer una mayor transferencia de información y permitir que se guarden cantidades de gran magnitud de información con un alto nivel de redundancia. En la Figura 6 se observa el ejemplo de un modelo de almacenamiento basado en SAN (Axis Comunicactions Corp., 2018).

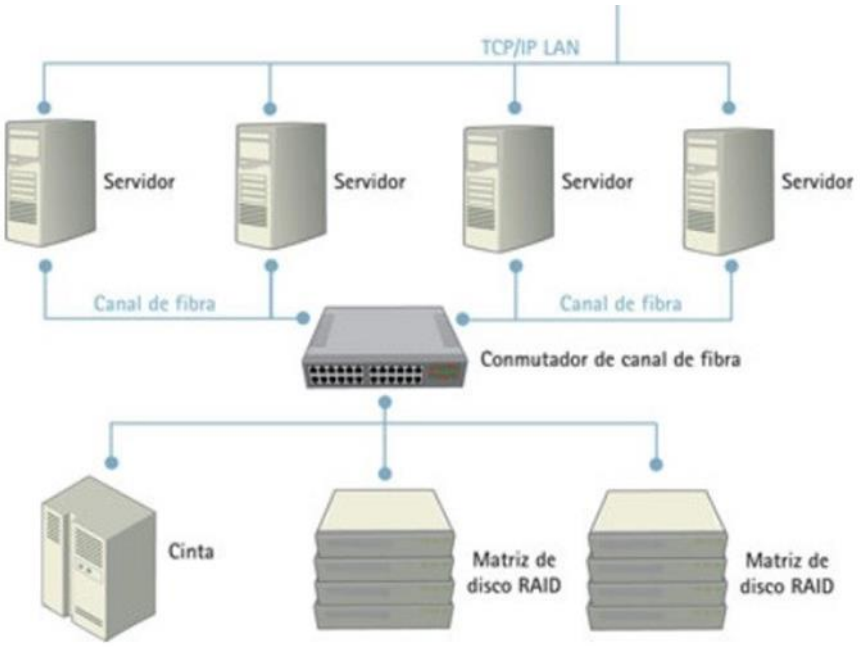


Figura 6. Arquitectura de red de almacenamiento por área (SAN)

Fuente: Sistemas de gestión de video (Axis Comunicactions Corp., 2018).

2.2.6.2. RAID

Redundant Array of Independent Disks (RAID) o en español matriz redundante de discos independientes, es la fusión de varios discos duros en donde el sistema operativo reconoce como un gran disco duro, una de las características principales es la alta redundancia que posee en caso de que se averíe un disco del conjunto en total. Existen varios arreglos de discos desde cero redundancias hasta la completa protección a fallas sin perder ningún solo dato en averías de discos duros. En la Figura 7 podemos observar un ejemplo de del diseño basado en RAID (Axis Comunicactions Corp., 2018).

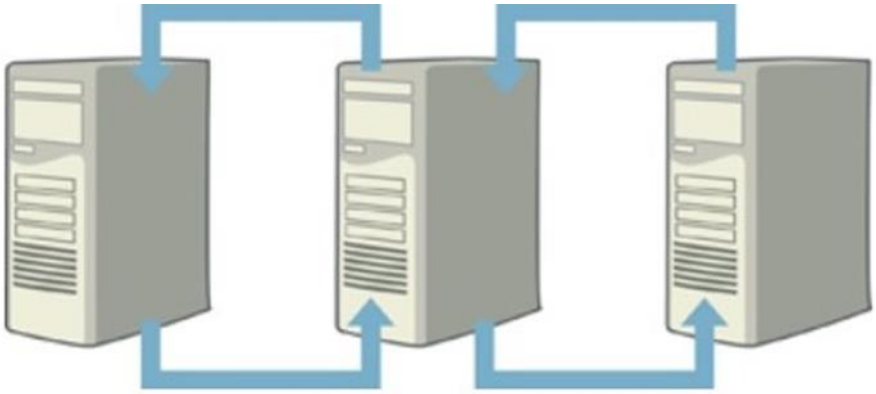


Figura 7. Replicación de datos

Fuente: Sistemas de gestión de video (Axis Comunicactions Corp., 2018).

2.2.7. Servidores de centrales de video

Son servidores dedicados y exclusivamente diseñados para centrales de video las cuales tienen la capacidad de controlar múltiples pantallas, estos servidores cuentan con entradas y salidas integradas. Es decir, un servidor de cuatro tarjetas permite construir paredes de video de hasta 16 entradas HD en 16 salidas HD. Los servidores están construidos con un hardware especial para proporcionar una buena refrigeración y cuenta con opciones adicionales para la alimentación redundante (Axis Comunicactions Corp., 2018),

2.2.8. Mural de video

El mural de video o también llamado videowall es un sistema de varias pantallas unidas en un mural (video proyectores, monitores, panales TVs o LED), las cuales producen contenido multimedia de manera unificada. El sistema simula una gran pantalla de grandes proporciones. Entre los usos de los videowalls se puede apreciar los siguientes: panales publicitarios (aplicación comercial), la creación de pantallas gigantes, paneles informativos (ejemplo: estadísticas, comunicaciones sobre abordaje y desembarco en aeropuertos, etc.), etc. Su aplicación depende a la demanda y es demasiada extendida. Las pantallas o monitores del videowall se puede colocar en forma uniforme, esto quiere decir, que las pantallas están distribuidas en idénticos tamaños de manera matricial, bien formado en un mural plano o bien curvo (con

configuración AxB, donde A es filas y B es pantallas), o también de diseño desordenado, con pantallas diferentes o de iguales tamaños y en diferentes orientaciones. El cual tiene como objetivo exhibir uno o varias piezas multimedia, entre videos, imágenes, etc. (Salvador, Boronat, Montagud, & Marfil, 2017). En la Figura 8 podemos observar dos ejemplos de diseño del videowall.

Figura 8. Videowall parejo plano (izquierda) y desigual (derecha)

Fuente: Sistema videowall de bajo coste basado en raspberry pi, personalizable y configurable dinámica y remotamente (Salvador, Boronat, Montagud, & Marfil, 2017).

2.2.9. KVM

ATEN International Co. Ltd. (2019) Indica. El extensor de KVM (keyboard, video & mouse) tiene la función de conectar remotamente un ordenador en cualquier otra ubicación que se requiera sin la necesidad de trasladar el equipo, esta conexión se realiza a través de IP la solución está conformada por dos consolas una de transmisión y la otra de recepción. En la Figura 9 podemos observar el diagrama de diseño de los KVM.

Figura 9. Diagrama de un Extensor KVM a través de IP

Fuente: Autoría propia

2.2.10. Arquitectura de Federación

Genetec Inc., (2019) Indica. Es una arquitectura o modelo que se usa cuando se tienen sitios separados geográficamente, la tecnología de federation brinda la posibilidad de reducir el consumo de ancho de banda del sistema de video vigilancia usando una solución de video a demanda, esto quiere decir que solo se transmitirá cuando el operador lo solicite en el resto de los casos no se trasmitirá, pero la grabación continuara localmente. Cada sistema es independiente a la central y la arquitectura de federation une todos estos sistemas en un entorno global, pero manteniendo sus independencias. En la Figura 10 se muestra el modelo de federación.

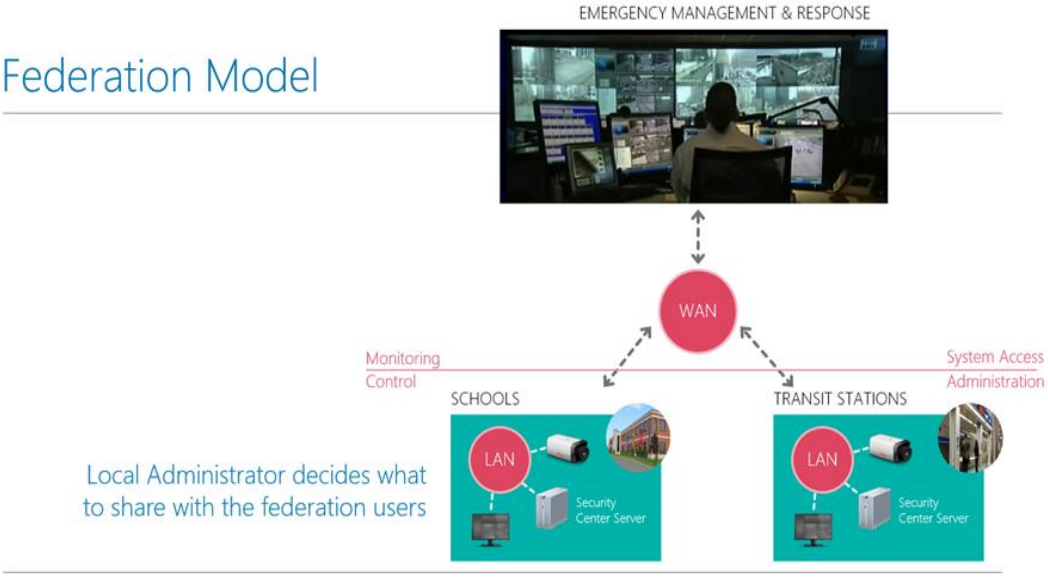


Figura 10. Modelo de federación

Fuente: SC-SDC-001 Certificación de diseños de sistemas Genetec Inc., (2019).

2.2.11. Verificación y validación de diseño y desarrollo

Verificación y validación son unos conceptos menos comprendidos de las buenas prácticas de diseño en ISO 9001, existe diferencia entre la Verificación del Diseño y la Validación del Diseño. Estos dos conceptos son diferentes, e importantes para un buen proceso de diseño (Hammar, 2015).

2.2.11.1. Verificación de diseño y desarrollo

Hammar (2015) La etapa de verificación consiste en reunir información del producto o productos (antes y después), para poder comprobar las nuevas características del producto final y verificar. En esta etapa se verifica que se está cumpliendo con todos los cambios establecidos en el diseño identificados como elementos de entrada.

2.2.11.2. Validación de diseños y desarrollo

Hammar (2015) indica que en la etapa de validación consiste en la revisión del prototipo o producto final, en otras palabras, confirma si efectivamente los cambios declarados como elementos de entrada en el producto tiene la satisfacción del cliente o usuario final.

2.2.12. Análisis de Reducción de incidentes

El análisis de reducción de incidentes se mide a través de los indicadores clave de rendimiento (KPI por sus siglas en inglés) proporcionan a la industria una posibilidad de medida que examina la productividad respecto de algún objetivo. El uso de KPI es común en las organizaciones para medir la calidad y el éxito de sus objetivos, o la entrega final de productos y servicios (Villa, 2015).

2.2.13. Estado antes de la Implementación

El Centro de Comando, Control y Comunicación (C4) tiene una infraestructura instalada como base y es propiedad de la Policía Nacional del Perú (PNP), el C4 integra diferentes sistemas de video de las Municipalidades e Instituciones de Seguridad Pública. Actualmente varias soluciones tecnológicas y equipos se encuentran deshabilitados (licencia caducada) o averiados (falta de mantenimiento), se utilizarán los recursos tecnológicos y la infraestructura existente tales como (hardware, softwares, etc.). El antiguo C4 pasará por una restructuración y se convertirá en el nuevo Centro de Operaciones de Seguridad (COS) y funcionará a Nivel Operacional durante el crecimiento de los Juegos Panamericanos Lima 2019. En la tabla 1 se detalla la infraestructura del C4.

Tabla 1. *Relación de software y hardware del C4.*

Ítem	Equipos	Cantidad	Marca
A	**APLICACIÓN / SOFTWARE**		
A1	Video Wall	1	Mura Control
A2	Video Wall	1	Hyperwall
A3	Controlador Dominio	1	CISCO
A4	Servidor Control Acceso	1	ISE
A5	Sistema Grabación de Llamadas	1	Mediasense
A6	Sistema de Telefonía	2	Cisco Unified
A7	Sistema Mensajería	2	Cisco Unified
A8	Sistema Voice Mail	2	Cisco Unity
A9	Sistema Gestión Equipos Red	1	Cisco
A10	Software de Virtualización	1	VMware
B	**VIRTUAL MACHINE**		
B1	Servidor Grabación Video	5	ISS

B2	Servidor Control Acceso	1	ISE
C	**SERVIDORES / CHASIS**		
C1	UCS (A / B)	2	AD, DHCP, DNS, IM Visión APICSA
C2	ESXI	4	Host VMware de VMs
C3	UCS-VM	2	Sistema Telefonía IP
C4	Servidor Blade	4	CISCO
C5	Chasis Cisco 4 Servidores blade	1	CISCO
C6	Fabric InterConnect	2	CISCO
D	**SISTEMA STORAGE Y BACKUP**		
D1	Storage de Almacenamiento	1	EMC2
D2	Servidor Backup en Cinta	2	HP
D3	Consola Gestión Storage	3	Backup Storage
E	**NETWORKING**		
E1	Switch Core	2	CISCO NEXUS 7700
E2	Switch Distribución	2	CISCO
E3	Fabric InterConnect	2	Switch Chasis Cisco
E4	UCS Manager	1	CISCO UCS
E5	Switch Acceso	5	CISCO Catalyst 3850
E6	Wireless WLC	1	CISCO 2500 Series
E7	Gateway de voz	2	CISCO 3925-CHASIS
E8	Router Acceso	2	CISCO ASR 1000
F	**SEGURIDAD PERIMETRAL**		
F1	Consola Gestion Firewalls	1	Smart-1 210
F2	Seguridad Perimetral (Firewall)	2	CheckPoint
F3	Sistema prevención Intruso	4	IPS MCAfee
G	**COMPUTADORA PERSONAL**		
G1	Ordenadores	23	HP
G2	Monitores	42	PELCO
H	**VIDEOWALL**		
H1	Controlador SENECA	1	SENECA
H2	Tarjetas Matrox	1	Matrox
H3	Monitores de 55 pulgadas (incluyendo racks)	19	Samsung
I	Teléfono IP	17	CISCO
J	Teléfono IP	5	CISCO
K	Teléfono IP	3	CISCO
L	MiniPC Gigabits	4	
M	Servidor	1	GENETEC
N	Monitor LED	12	IIYAMA
O	Pizarra interactiva StarBoard	2	PROMETHEAN/HITACHI

P	**APC SCHNEIDER SYMMETRA PX**		
P1	Cámaras	6	APC
P2	Switch Port	1	APC
P3	Switch Rack Monitor	1	APC
P4	Switch Rack Monitor	1	APC
P5	Aire Acondicionado de Precisión	1	APC
P6	UPS	1	APC
P7	Power Distribution Unit (PDU)	1	APC
P8	Power Module	3	APC
P9	System Supply Power	1	APC
P10	Intelligence Module	2	APC
P11	XR Baterry Enclosure	16	APC
Q	Adaptadores de videos, Cables HDMI	20	
R	PoE-Switch	1	HP
S	PoE-Switch	1	HP

Fuente: Autoría propia

Por motivos de seguridad no se mostrará las versiones y modelos específicos, por que atentan contra la seguridad del centro de operaciones de seguridad.

CAPÍTULO III
DESARROLLO DE LA SOLUCIÓN

3.1. Diagrama de Bloques

En este capítulo se describe el desarrollo del diseño y la implementación del proyecto, en la Figura 11 se detalla el diagrama de bloques que describe paso a paso los niveles de ejecución del proyecto. Como primer paso comenzamos con el 3.1.1. Adquisición del software y hardware. Luego procedemos con el segundo paso 3.1.2. Instalación del hardware, en este nivel contiene subprocesos las cuales son: 3.1.2.1. Instalación del servidor seneca; 3.1.2.2. Instalación del cableado del servidor seneca; 3.1.2.3. Instalación de los KVM aten serie KE6940 y 3.1.2.4. Instalación del cableado del KVM. Procedemos con el tercer paso 3.1.3. Instalación del software, en este nivel contiene subprocesos las cuales son: 3.1.3.1. Instalación del mural de video matrox; 3.1.3.2. Configuración del mural de video matrox; 3.1.3.3. Instalación de la plataforma de video genetec y 3.1.3.4. Configuración del security center genetec. Continuamos con el cuarto paso 3.1.4. Arquitectura de federación. Procedemos con el quinto paso 3.1.5. Verificación y validación. Como sexto y último paso 3.1.6. Análisis de incidentes.

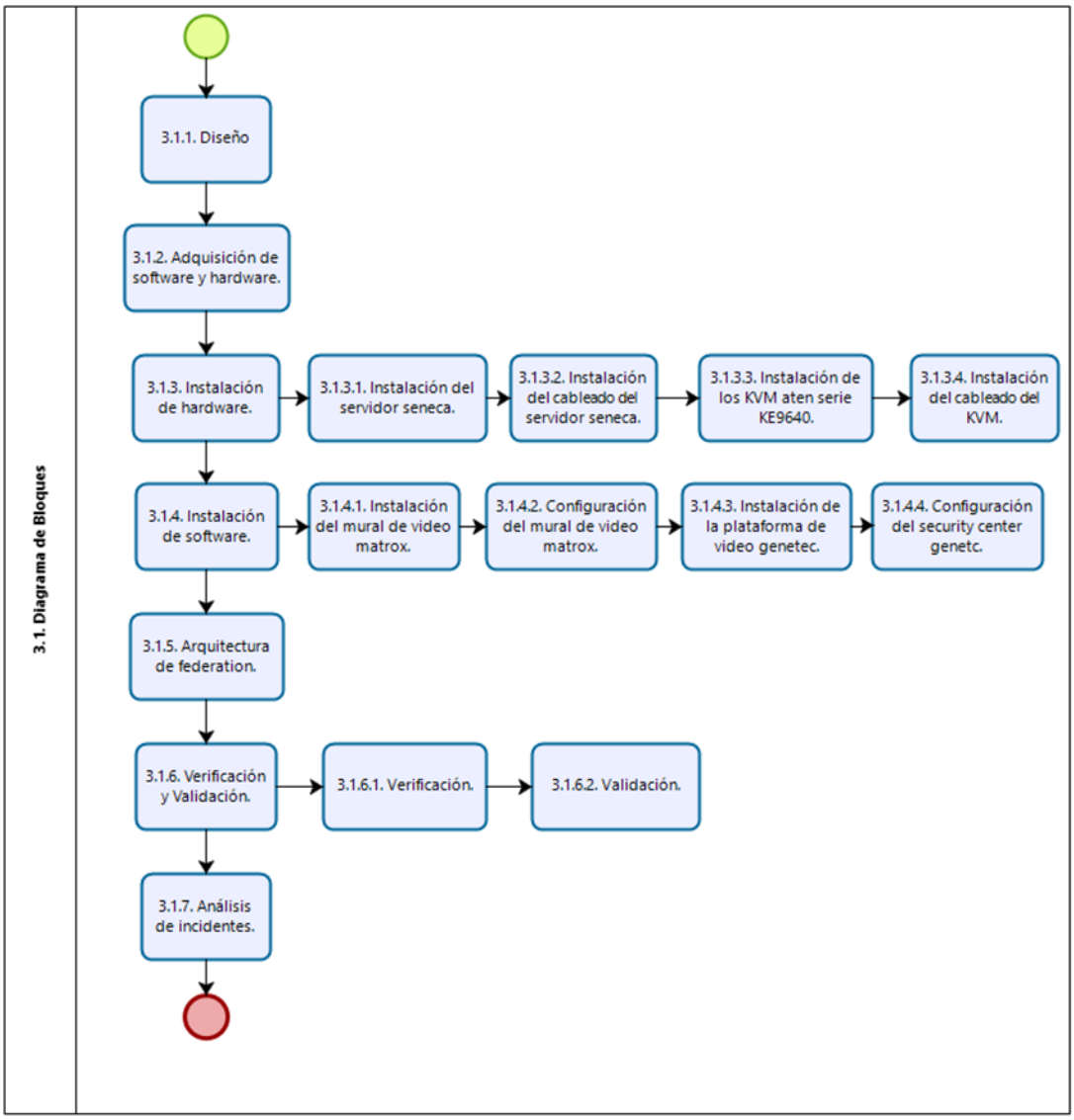


Figura 11. Diagrama de bloques

Fuente: Autoría propia

3.1.1. Diseño del centro de Monitoreo

Se diseña un centro de monitoreo en un lugar del anterior C4, el cual debe ser adaptado para garantizar su funcionamiento de acuerdo con las especificaciones indicadas en este documento.

El centro de monitoreo tendrá las siguientes tareas básicas como funciones básicas:

- Almacenamiento de imágenes del sistema de monitoreo de video y eventos de alarma obtenidos a través de un enlace de comunicación;
- Almacenamiento de las imágenes de respaldo de los DVR de los edificios obtenidas mediante transferencia de archivos a través de dispositivos físicos o mediante el enlace de comunicación, considerando la transferencia de todas las imágenes de todas las unidades durante un período mínimo de 3 meses de grabación.
- Gestión de dispositivos de telemetría, sensores y equipos de red activos, monitoreando el estado operativo de cada unidad.
- Control, a través de equipos de profesionales, especialmente capacitados para operar todos los recursos instalados, monitoreando así todas las unidades las 24 horas, los 7 días y los 365 días;
- Registro de usuarios y grupos para operar el sistema de video monitoreo, alarma y control de acceso en las unidades y en el centro de monitoreo; ambiente del centro de monitoreo y también en ubicaciones, del tipo rack 22", y se deben utilizar los racks existentes en cada unidad. Deben adoptarse medidas para garantizar la no violación del rack, como la colocación de llaves, rejillas metálicas u otro sistema para no permitir el retiro de los dispositivos de grabación de imágenes del lugar.

Se debe considerar la necesidad de realizar todos los ajustes eléctricos necesarios, para que exista una completa y perfecta operacionalización de sus servicios (circuitos de salida secundarios y primarios, aires acondicionados lámparas adecuadas, sistemas eléctricos contra interrupciones de energía y similares). Todos los circuitos de alimentación instalados deben instalarse en cuadros de distribución eléctrica, debidamente identificados como parte de la solución de vigilancia y electrónica. En el ambiente del centro de monitoreo, se deben instalar circuitos que permitan el funcionamiento de una red estabilizada protegida por un UPS de al menos 5 kVA.

En el ambiente del centro de monitoreo se deben instalar dispositivos que garanticen la seguridad del sitio, como cámara de video vigilancia en la puerta de acceso y en el ambiente interno, control de acceso mediante identificación, con la respectiva autorización previa de acceso al sitio. Todos los profesionales involucrados deben estar registrados y capacitados en los procesos de uso del medio ambiente.

Todo el mobiliario debe estar disponible para la instalación de la sala de monitoreo con estricto cumplimiento de las normas de ergonomía con el fin de evitar daños a los profesionales.

Cada operador debe tener el siguiente equipo:

- Un teléfono;
- Un teclado y un mouse para controlar la estación;
- Un joystick para controlar cámaras móviles;
- Un micrófono y un altavoz conectados al sistema de CCTV para la comunicación inmediata con el sistema.
- Una computadora con tarjeta de video para 2 monitores de 22 pulgadas con software de gestión del sistema de monitoreo de video que muestra información como: hora de alerta del evento, nombre del evento, edad del crítico, código del equipo que registró el evento, reproducción del evento. Todo el monitoreo por video debe realizarse en estos dos monitores, uno específico para cámaras móviles y otro para el acceso a los DVR de cada sede.

Para el montaje de la sala se debe considerar como mínimo el siguiente equipamiento:

- 2 gabinete estándar de 19”, 43U, 800 mm de profundidad, como se describe en el ítem 3.2 - Equipo complementario
- 2 Mesa Ergométrica para 8 operadores, para alojar 16 monitores LCD de 22", teclados y mouse.
- 1 mesa de trabajo ergométrica para 1 supervisor
- 16 silla ergonómica, ajustable, con brazos y ruedas

- 1 aire acondicionado de techo / pared dividido, 30.000 BTU, 220 V
- 1 control de acceso biométrico con cerradura de puerta de metálica, software de registro

3.1.2. Adquisición de software y hardware

Como primer paso adquirimos los softwares y el hardware necesario para el desarrollo de nuestra solución, como ya se cuenta con una infraestructura base solo se modificarán los softwares y hardware necesarios para la implementación del nuevo Centro de Operaciones de Seguridad (COS).

A continuación, se muestra en la Tabla 2 el software adquirido en el cual se describe la marca, el modelo y la cantidad de unidades.

Tabla 2. *Relación del hardware adquirido.*

RELACIÓN DE HARDWARE					
ITEM	**MARCA**	**MODELO**	**DESCRIPCIÓN**	**UNIDAD**	**TOTAL**
1	SENECA	VWCMURA	Servidor	Und.	1
2	ATEN	KE6940T	Conmutador de teclado, video y mouse (KVM-Tx)	Und.	16
3	ATEN	KE6940R	Conmutador de teclado, video y mouse (KVM-Rx)	Und.	16

Fuente: Autoría propia.

Luego, se muestra en la Tabla 3 el software adquirido en el cual se describe la marca, la versión y la cantidad de licencias.

Tabla 3. *Relación del software adquirido*

RELACIÓN DE SOFTWARE					
ITEM	MARCA	MODELO	DESCRIPCIÓN	UNIDAD	TOTAL
1	GENETEC	Security Center	Sistema de Gestión de Video	Und.	1
2	Matrox	Mura Control	Mural de Video	Und.	1

Fuente: Autoría propia

3.1.3. Instalación de Hardware

Seguimos con el segundo paso el cual es la instalación física del hardware donde también describiremos sus características técnicas, luego pasaremos a la instalación del cableado de acuerdo con el diseño planteado para nuestra solución

3.1.3.1. Instalación del servidor Seneca

Procedemos con la instalación del servidor Seneca el cual la marca ofrece la experiencia y tiene los recursos para construir controladores de Videowall optimizados mediante la asociación con los principales fabricantes de tarjetas de vídeo y proveedores de plataformas de software independientes. En nuestra solución usaremos el servidor seneca VWC-PLUS, en la Tabla 4 se muestra sus características técnicas, en el Anexo 1, Figura 24 se muestra la imagen del servidor seneca instalado.

Tabla 4. *Relación del software adquirido*

Procesador	6ta gen Intel Core i7-6900X Procesador 4.0GHz
Sistema Operativo	Windows 10 Profesional
Fabricante	Seneca
Gráficos	Opciones de GPU discretas validadas de AMD, Matrox, y NVIDIA
Capacidad	Hasta 32 pantallas
Reproducción de medio de un monitor	4K; 2160p60fps
Reproducción de medio de varios monitores	28 x 4K; 2160p60fps
Orientación	Paisaje y retrato
Salida de Video	Opciones de GPU discretas validadas de AMD, Matrox, y NVIDIA
Audio	Sonido envolvente 5.1 integrado. (7.1 opcional)
Storage	1TB HDD (Hasta 24TB)
	1 x M.2 Sata 6GB/s
Unidad Óptica	24x DVDRW (opcional BluRay)
Memoria	Hasta 128GB DDR4 2133MHz
Conectividad	LAN 1: Intel I210-AT, Gigabit LAN Controlador
	LAN 2: Intel I218LM, Gigabit LAN

	Interconexión dual entre el controlador de acceso a medios integrados (MAC) y la capa fisica (PHY)
USB	12 x USB 2.0 (2 front, 10 back)
Capacidad de expansión	2 x RJ45
	2 x eSATA 6Gb/s
	1 x S/PDIF Optical
	Dual 10Gb/s SATA Express
	32Gb/s M.2 x4 Speed
	Q-Code logger/USB BIOS Flashback
	8-Channel audio with DTS
Ranura de expansión	7 x PCIe 3.0/2.0 x16
	(single x16; dual x16/x16; triple x16/x16/x16; quad x16/x16/x16/x16; seven x16/x8/x8/x8/x8/x8/x8)

Fuente: *VWC-PLUS star guide* (Arrow Electronics, Inc., 2018)

3.1.3.2. Instalación del cableado del servidor seneca

A continuación, instalamos el cableado de acuerdo con el diseño mostrado en la Figura 12, se observa que el cableado tiene dos tramos desde el servidor Seneca, el tramo 1 conecta los gabinetes hacia el servidor seneca y el tramo 2 conecta el servidor Seneca hacia el mural de video.

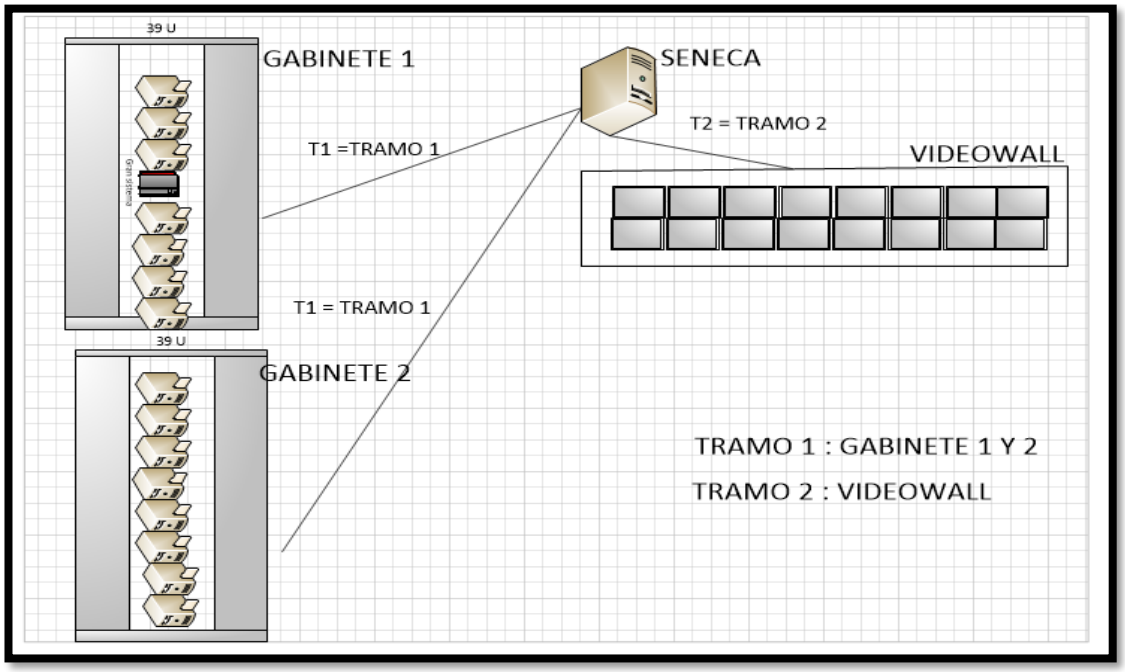


Figura 12. Diseño del Cableado tramo 1 y 2

Fuente: Autoría propia

Ejecutamos la instalación del cableado del tramo 1, en la Figura 13 se muestra el diseño de instalación que conecta el servidor Seneca con los 16 ordenadores, con una conexión de video directa a través del cable DVI. Los ordenadores están agrupados en dos gabinetes cada uno contiene 8 ordenadores. En el Anexo 2, Figura 25 - 26 se muestran las imágenes de los ordenadores.

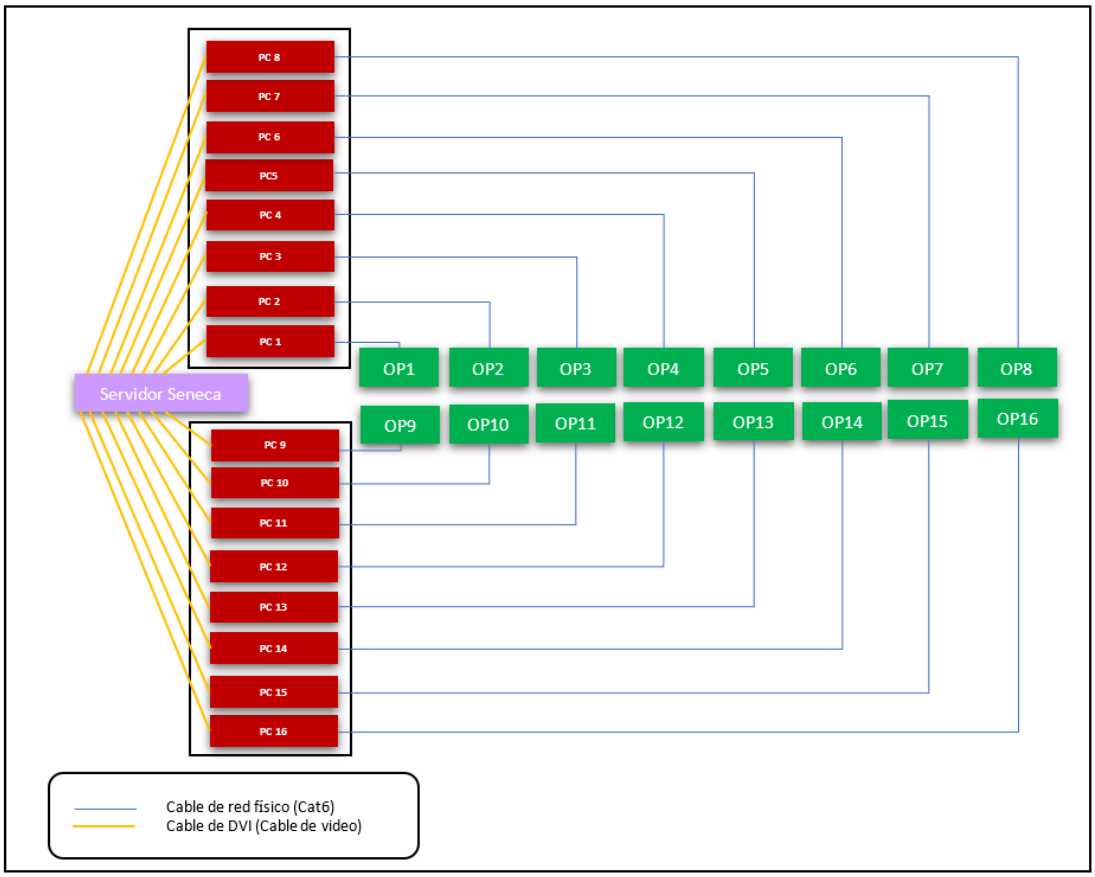


Figura 13. Diseño del cableado del tramo 1

Fuente*:* Autoría propia.

Continuamos con la instalación del cableado del tramo 2, en la Figura 14 se muestra en el diseño del cableado del tramo 2 el cual está instalado con cable HDMI desde el servidor Seneca hacia el mural de video. En el anexo 3, Figura 27-29 se muestran la instalación del cableado desde el servidor seneca

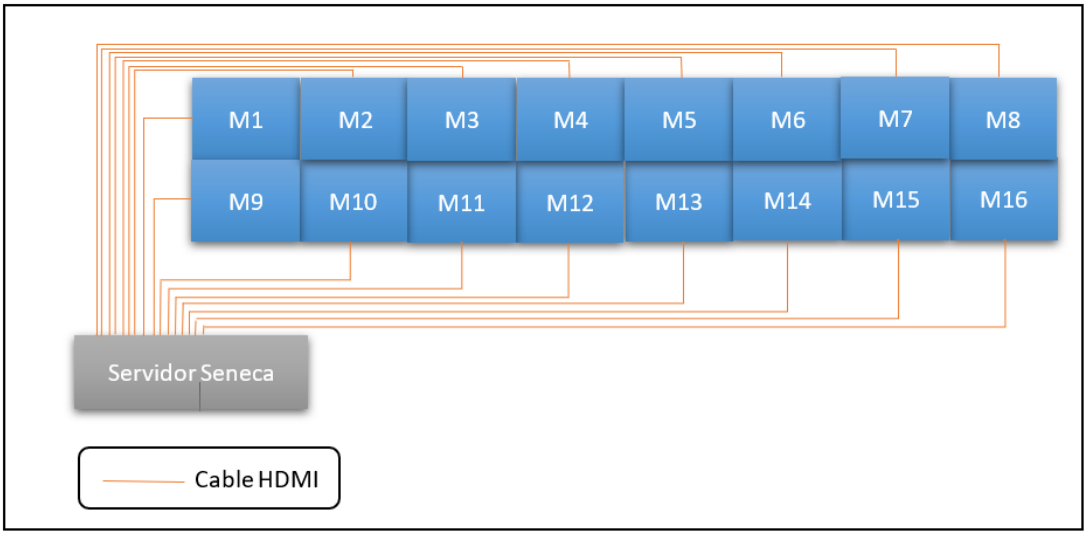


Figura 14. Diseño del cableado del tramo 2

Fuente: Autoría propia.

3.1.3.3. Instalación de los KVM aten serie KE6940

Procedemos con la instalación de los KVM ATEM serie KE6940, Los KVM están compuestos por 2 unidades: transmisión y recepción. La consola de transmisión se conecta al ordenador y la consola de recepción se puede ubicar en un lugar remoto para un mejor uso del área o sala de instalación donde se instalarán los operadores. La comunicación entre consolas se realiza por medio de una red TCP/IP, el medio físico de conexión es por cable UTP Cat6A. El tipo de arquitectura utilizada es de punto a punto. En la Tabla 5 se muestra las características técnicas del KVM trasmisor y receptor.

Tabla 5. Relación de software y hardware del C4.

	KE6940R	**KE6940T**
Puerto USB	2 x USB Tipo A hembra (Blanco)	2 x USB Tipo A hembra (Blanco)
Puertos de consola	2 x USB Tipo A hembra (Blanco)	2 x USB Tipo A hembra (Blanco)
	2 x DVI-I hembra (Blanco)	2 x DVI-I hembra (Blanco)
	1 x Mini conector estéreo (Verde)	1 x Mini conector estéreo (Verde)
	1 x Mini conector estéreo (Rosa)	1 x Mini conector estéreo (Rosa)
	1 x DB-9 macho (Negro)	1 x DB-9 macho (Negro)
Alimentación	1 x Conector de CC (Cat5e)	1 x Conector de CC (Negro)
Puertos LAN	1 x RJ-45 (Cat6A)	1 x RJ-45 (Cat6A)

Puertos KVM	N/D	1 x USB Tipo B hembra (Blanco)
		2 x DVI-I hembra (Blanco)
		1 x Mini conector estéreo (Verde)
		1 x Mini conector estéreo (Rosa)
		1 x DB-9 hembra (Negro)

Fuente: Autoría propia

Se procede a configurar los KVM colocando una IP en cada una de las consolas, tanto en el trasmisor como en el receptor, por motivos de seguridad no se mostrará las IPs asignadas y no se describirá los detalles de la configuración. En el Anexo 4, Figura 30-31se muestran las imágenes de la instalación física.

3.1.3.4. Instalación de cableado del KVM

A continuación, instalamos el cableado de acuerdo con el diseño mostrado en la Figura 15. Se observa los gabinetes 1 y 2, el cual alberga los ordenadores y las consolas de transmisión las cuales están conectadas vía cables de video multimedia, la consola de transmisión está conectada con la consola de recepción vía cable UTP Cat6A y en la consola de recepción se instala el teclado, mouse y dos pantallas para el uso de los operadores. En el Anexo 5, Figura 32-33 se muestran las imágenes de instalación del cableado del KVM.

Figura 15. Diseño del cableado de los KVM receptor y transmisor

Fuente: Autoría propia

3.1.4. Instalación de Software

Seguimos con el tercer paso el cual es la instalación del software, donde describiremos sus características técnicas, luego pasaremos a la configuración del software de acuerdo con los requerimientos planteados en nuestra solución

3.1.4.1. Instalación del mural de video matrox

A continuación, instalamos el videowall de matrox el cual nos ayudará a controlar las 16 pantallas instaladas en el mural, para poder crear matrices de

pantallas según sea el caso requerido. Los operadores podrán realizar las siguientes funciones en el software videowall matrox:

- Ejecución del software de forma local y remota.
- Crear, salvar, renombrar, copiar y eliminar plantillas.
- Importar o exportar plantillas.
- Posicionar, redimensionar, cortar y etiquetar ventanas en cualquier lugar del video Wall
- Renombrar, cortar, rotar, y aplicar color, texto superpuesto, y aplicar filtros de entrelazado a los contenidos de las fuentes.
- Aplicar parámetros de corrección a las fuentes específicas como matiz, saturación, brillo, y contraste de color.
- Agregar y controlar aplicación externa, así como VLC, VNC, y Microsoft PowerPoint, página web, fuente HTML5 e imágenes sobre el video Wall.
- Crear plantillas programadas para que automáticamente cambien de una a otra.

El software Matrox MuraControl para Windows, se instala en el controlador Seneca, con una licencia USB dongle. Procedemos con la asignación de una dirección IP, puerto y password, por motivos de seguridad no se va a describir el proceso de instalación del software mural control. En la Figura 16 observamos la interfaz gráfica del software matrox muracontrol, el cual fue instalada con éxito en el controlador seneca.

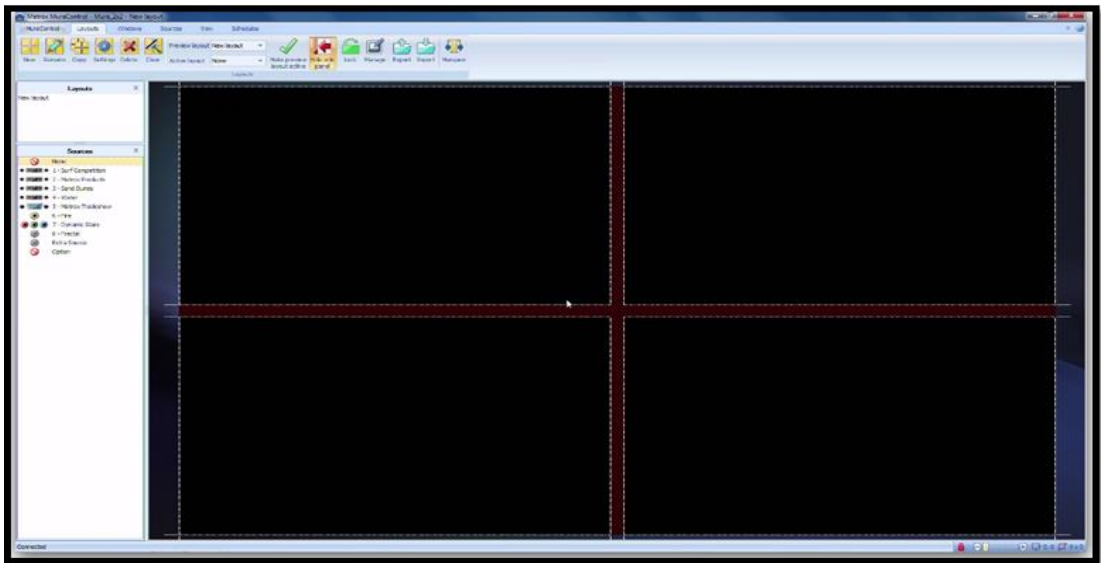


Figura 16. Interfaz gráfica Matrox MuraControl para Windows

Fuente: Matrox mural control for Windows user guide (Matrox Graphics, Inc, 2017)

3.1.4.2. Configuración del mural video matrox

Se procede a configurar el software matrox mural control con la plantilla creada para nuestra solución, la plantilla fue diseñada usando una matriz de 2x8 la cual es la distribución de las pantallas del mural de video. En la Figura 17 se puede observar la interfaz del software con la configuración de la plantilla y la matriz 2x8. En el Anexo 6, Figura 34 – 39 se muestran las imágenes de la configuración del mural de video matrox,

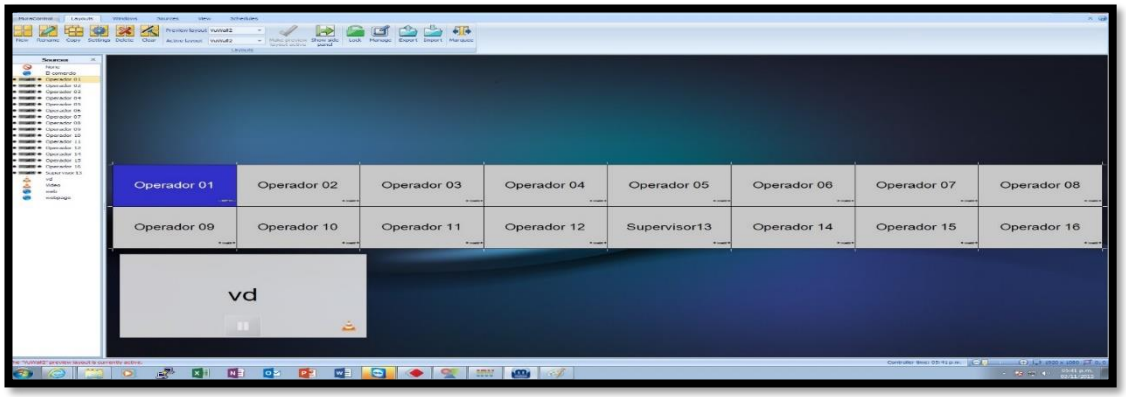


Figura 17. Plantilla de la matriz 2x8

Fuente: Autoría propia

Luego procedemos a asignar a cada operador una pantalla como se observa en la Figura 18

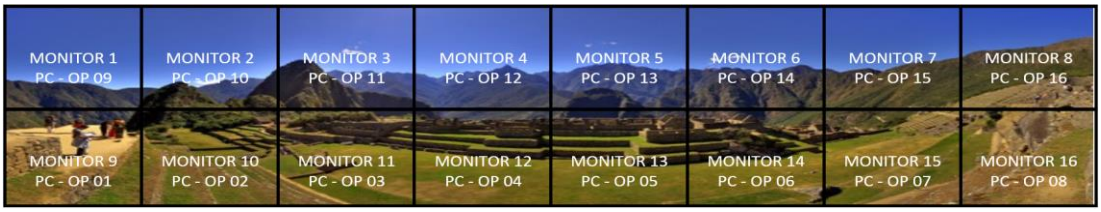


Figura 18. Distribución de cada monitor asignado a cada operador

Fuente: Autoría propia

3.1.4.3. Instalación de la Plataforma de video genetec

A continuación, procedemos a instalar la plataforma de video genetec. En nuestra solución aremos uso de 4 servidor virtuales (servidor de security center, servidor archive, servidor movile y servidor federation) los cuales estarán alojados en la infraestructura perteneciente a la PNP, los 4 servidores virtuales tienen las mismas características recomendadas por el fabricante para el óptimo funcionamiento del software. Para este proyecto, se adquirió una licencia Enterprise security center 5.7 para el uso de su plataforma unificada con la restricción de algunos servicios (cada servicio tiene licencia independiente). Los servicios adquiridos son directory, archiver, access manager, mobile y federation.

Por motivos de seguridad no se entrará en detalles de la instalación del servidor virtual con el software genetec.

3.1.4.4. Plataforma de hardware

Se procede a la configurar el servidor security center, este servidor brinda los servicios de directory y access manager. A continuación, se describe las siguientes consideraciones:

- El Directory soportara hasta 1 millón de entidades y hasta 1000 conexiones de clientes concurrentes.
- Soportara hasta 1000 eventos/seguridad o 1000 alarmas/seguridad.
- El sistema soportara 761 cámaras.

A continuación, procedemos a configurar el servidor archive. El servicio archive es parte del sistema security center el cual se configura para soportar las siguientes consideraciones:

- El sistema soportara como mínimo 761 cámaras.
- Las resoluciones/codec de resolución serán H264 y H265.
- La velocidad mínima de grabación será de 15 fps.
- El ancho de banda por cámara será de 2 Mbps.
- El tiempo de grabación será continúa las 24 horas y 7 días de la semana.
- El periodo de retención de información de video será de 7 días (la grabación será de manera local y solo se trasladará a la central los videos a demanda).
- El almacenamiento será redireccionado al servidor NAS propiedad de la PNP el cual contiene 50 Terabytes de almacenamiento.

Procedemos a configurar el servidor mobile, esta función brinda a los celulares la opción de ser cámaras de video vigilancia móviles y tiene la capacidad de trabajar tanto en Android como en IOS. El número máximo de conexiones móviles es de 50 usuarios activos, usa la resolución de las cámaras como fueron configuradas en el security center y el tras codifica en resoluciones móviles 320x240.

Por motivos de seguridad no se entrará en detalles en la configuración de los servicios del software genetec.

3.1.5. Arquitectura de Federation

Como cuarto paso en nuestra solución se propone la arquitectura de federation, el cual es ideal para un gran número de sitios separados geográficamente, como es nuestro caso con las diferentes sedes deportivas. A continuación, los requisitos para la federation:

- Requiere licencia de Enterprise

- Se puede federar a tres versiones anteriores de Security Center (SC), una versión posterior (Ejemplo: v.5.6 puede federar v.5.7, v. 5.6, v. 5.5, v. 5.4, v 5.3).
- No hay límites cuantas veces puedes federar un sistema.
- Solo soporta dos niveles de federación: secundario y primario o principal
- Cuando esta federado con los dos niveles de federación, el límite es de 75, 000 cámaras a nivel principal.

Procedemos con la configuración del servidor federation con la consideración de integrar 15 sedes, cada sede deportiva tiene instalado un NVR de la marca genetec y es independiente. El cual es compatible con la función federation de la plataforma de video de security center, se conecta de forma directa con el Centro de Operaciones de Seguridad (COS), estas sedes tienen una configuración independiente, pero se integran al COS convirtiéndose en una plataforma globalizada. En la siguiente Figura 19 se muestra el diagrama de integración usando la arquitectura de federación, al COS se integran 15 sedes deportivas de los juegos panamericanos. En el Anexo 7, Figura 40 – 52 se muestran las imágenes de los resultados de conexión con cada sede deportiva.

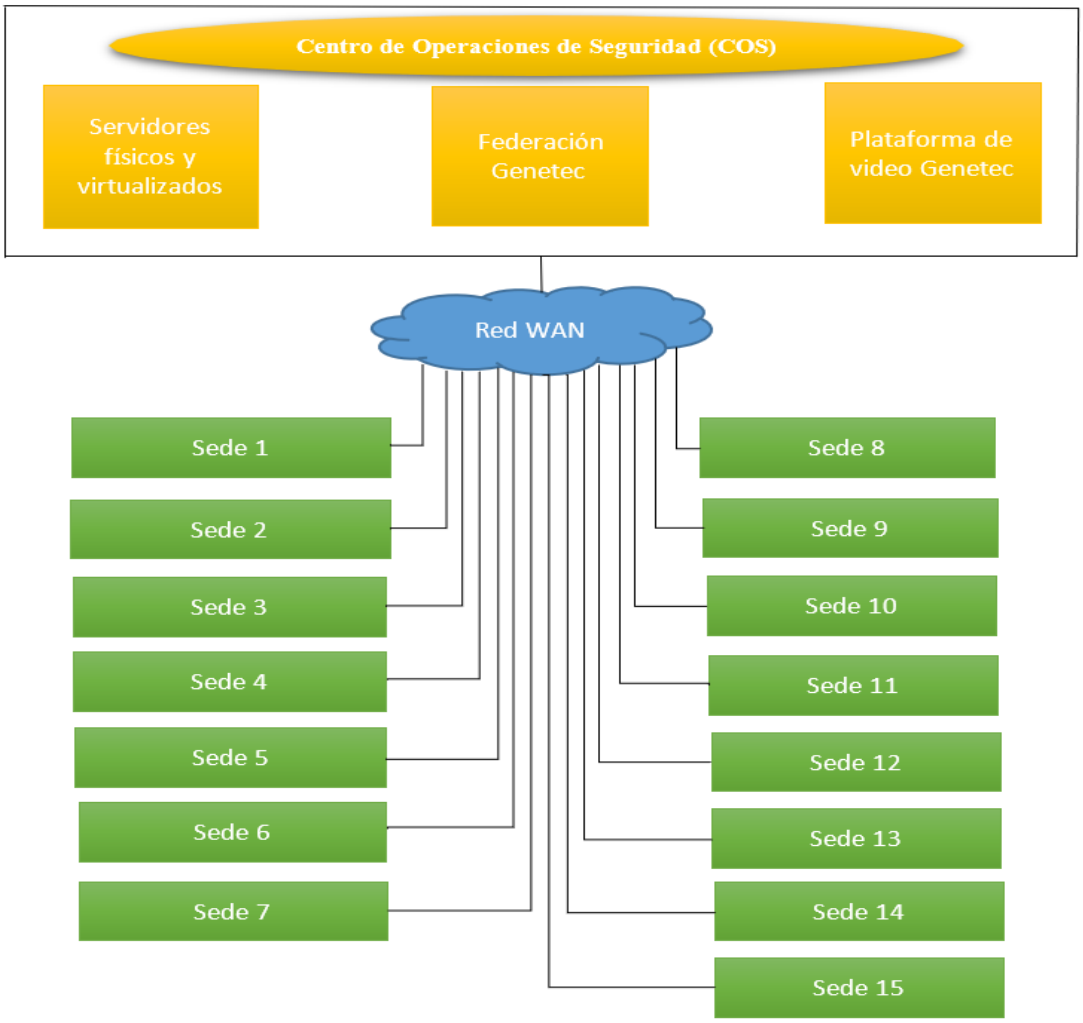


Figura 19. Arquitectura de federación de los juegos panamericanos

Fuente: Autoría propia.

3.1.6. Verificación y validación

A continuación, pasamos al quinto paso procedemos con la verificación y validación, usamos las recomendaciones de la ISO 9001 para poder verificar y validar. Procedemos a identificar los elementos de entrada, en nuestra solución los elementos de entrada son los hardware y software que se reemplazaron del Centro de Comando, control y comunicaciones (C4) para el desarrollo del nuevo Centro de Operaciones y Seguridad (COS).

3.1.6.1. Plataforma de hardware

La verificación la desarrollamos para ver si efectivamente lo ejecutado e instalado cumple con los elementos de entrada solicitados por él cliente.

A continuación, procedemos con la verificación del servidor seneca. Como se muestra en la Tabla 6 comparamos las características técnicas de la versión anterior con la versión actual instalada.

Tabla 6. Tabla técnica comparativa de los Senecas: VWC-4 y VWC-PLUS.

	Seneca VWC – 4	**Seneca VWC – PLUS**
Procesador	Intel Core i7, 3770K third generation processor.	Intel Core i7, 6950X 6th generation processor.
Graphics	Validate discrete GPU options from matrox and NVIDIA	Validate discrete GPU options from AMD, Matrox and NVIDIA
System memory	64 GB DDR3 1600 MHz	128 GB DDR4 2133MHz
Expansion slots	4PCIe x16 3.0/2.0 slots (dual x16 or x16, x8, x8 or quad x8 black and blue	7xPCIe3.0/2.0x16 (single x16; dual x16/x16; triple x16/x16/x16; quad x16/x16/x16/x16; seven x16/x8/x8/x8/x8/x8/x8)
Power supply	750W single power supply option for redundant power	Up to 1600W 80+Platinium Power Supply (Redundant Power Optional)

Fuente: Autoría propia

Procedemos a analizar las mejoras y verificamos que existen un incremento de 3 generaciones tecnológicas respecto a la versión anterior. El cual cumple y satisface con los requerimientos mínimos del cliente.

Siguiendo con el proceso de verificación pasamos al KVM receptor como se muestra en la Tabla 7 comparamos las características técnicas de la versión anterior y la versión actual.

Tabla 7. *Tabla técnica comparativa del KVM receptor.*

Receptor	**KE6940R**	**KE6940R v2.0**
Puerto USB	2 x USB Tipo A hembra (Blanco)	2 x USB Tipo A hembra (Blanco)

Puertos de consola	2 x USB Tipo A hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 macho (Negro)	2 x USB Tipo A hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 macho (Negro)
Alimentación	1 x Conector de CC (Cat5e)	2 x Conector de CC (Negro)
Puertos LAN	1 x RJ-45 (Cat5e)	1 x RJ-45 (Cat6a)
Puertos KVM	N/D	N/D

Fuente: Autoría propia

Procedemos a analizar las mejoras del KVM receptor y verificamos que existe un incremento en la velocidad de trasmisión de datos en la versión anterior soportaba máximo 1GB y la versión actual soporta hasta 10 GB. El cual cumple y satisface con los requerimientos de mínimos del cliente.

A continuación, seguimos con el KVM transmisor como se muestra en la Tabla 8 comparamos las características técnicas de la versión anterior y la versión actual

Tabla 8. *Tabla técnica comparativa del KVM receptor*.

Transmisor	**KE6940T**	**KE6940AT v2.0**
Puerto USB	2 x USB Tipo A hembra (Blanco)	2 x USB Tipo A hembra (Blanco)
Puertos de consola	2 x USB Tipo A hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 macho (Negro)	2 x USB Tipo A hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 macho (Negro)

Alimentación	1 x Conector de CC (Negro)	2 x Conector de CC (Negro)
Puertos LAN	1 x RJ-45 (Cat5e)	1 x RJ-45 (Cat6a)
Puertos KVM	1 x USB Tipo B hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 hembra (Negro)	1 x USB Tipo B hembra (Blanco) 2 x DVI-I hembra (Blanco) 1 x Mini conector estéreo (Verde) 1 x Mini conector estéreo (Rosa) 1 x DB-9 hembra (Negro)

Fuente: Autoría propia

Procedemos a analizar las mejoras del KVM transmisor y verificamos que existe un incremento en la velocidad de trasmisión de datos, en la versión anterior soportaba máximo 1GB y la versión actual soporta hasta 10 GB. El cual cumple y satisface con los requerimientos de mínimos del cliente.

Siguiendo con el proceso de verificación pasamos al software matrox mura control, en la Tabla 9 observarnos un cuadro comparativo de las mejoras de la versión anterior con la versión instalada actual.

Tabla 9. *Tabla comparativa del Matrox Muracontrol.*

Matrox MuraControl Versión 6.1	**Matrox MuraControl Versión 6.4**
En la versión 6.1, contiene el siguiente error: • Congelamiento del aplicativo cuando se realiza un arreglo (distribución de pantalla). El aplicativo se congelaba y se tenía que reiniciar perdiendo la configuración establecida. • Licencia activa	• En la versión 6.4 se corrige el error mencionado en la versión 6.1. y mejora el performance en un 10 % de la aplicación. • Nuevo Firmware que aumenta en 10% el performance de la aplicación. • Licencia renovada

Fuente: Autoría propia

Procedemos a analizar las mejoras y verificamos que existe corrección de errores respecto a la versión anterior e incrementa en un 10 % el performance de la aplicación. El cual cumple y satisface con los

requerimientos de mínimos del cliente. Siguiendo con el proceso de verificación pasamos al software genetec securtity center, en la Tabla 10 observamos la comparación de la plataforma de video genetec de su versión anterior con la versión actual instalada.

Tabla 10. *Tabla comparativa de Genetec Security Center.*

Genetec Version 5.5	**Genetec Version 5.7**
• **Microsoft® Windows 10 Pro/Enterprise** • **Microsoft® Windows 8.0/8.1 Pro/Enterprise** • **Microsoft® Windows 7 Pro/Enterprise/Ultimate SP1** • **Microsoft® Windows Server 2008 SP2** • **Microsoft® Windows Server 2008 R2 SP1** • **Microsoft® Windows Server 2012** • **Microsoft® Windows Server 2012 R2**	• Microsoft ® Windows 7 Pro/Enterprise/Ultimate SP1 • Microsoft ® Windows 8.1 Pro/Enterprise • Microsoft ® Windows 10 Pro/Enterprise • Microsoft ® Windows Server 2008 R2 SP1 • Microsoft ® Windows Server 2012 • Microsoft ® Windows Server 2012 R2 • Microsoft ® Windows Server 2016
• **SQL Server 2008 R2 Express/Standard/Enterprise** • **SQL Server 2012 Express/Standard/Enterprise** • **SQL Server 2014 Express/Standard/Enterprise**	• SQL Server 2008 R2 Express/Standard/Enterprise • SQL Server 2012 Express/Standard/Enterprise • SQL Server 2014 Express/Standard/Enterprise • SQL Server 2016 Express/Standard/Enterprise
• **Vmware ESXi 5.x** • **Vmware ESXi 6.x** • **Microsoft® Hyper-V con Windows Server 2012 o Windows Server 2012 R2**	• Vmware ESXi 5.x • Vmware ESXi 6.x • Microsoft ® Hyper-V con Windows Server 2012/2012 R2/2016 and SQL Server 2016
• **Licencia caducada**	• Licencia activa

Fuente: Autoría propia

Procedemos a analizar las mejoras y verificamos que existe un incremento en la capacidad de compatibilidad con nuevas versiones de servicios tecnológicos. El cual cumple y satisface con los requerimientos de mínimos del cliente.

3.1.6.2. Validación

A continuación, procedemos con la validación de la solución en general para observar si lo que se realizó cumple con las expectativas del cliente.

Procedemos a validar el funcionamiento del sistema del mural de video el cual constituye el funcionamiento del controlador seneca, funcionamiento del matrox mura control y la operatividad de las consolas kvms conectados a los módulos de usuarios. En la Figura 20 se muestra el mural de video configurado y observando videos remotamente de las diferentes sedes deportivas, también podemos validar que los operadores pueden visualizar las cámaras de las diferentes sedes deportivas. Los operadores están instalados y trabajando con las consolas kvm las cuales están conectados a los ordenadores y estos cuentan con conexión directa hacia el controlador seneca.

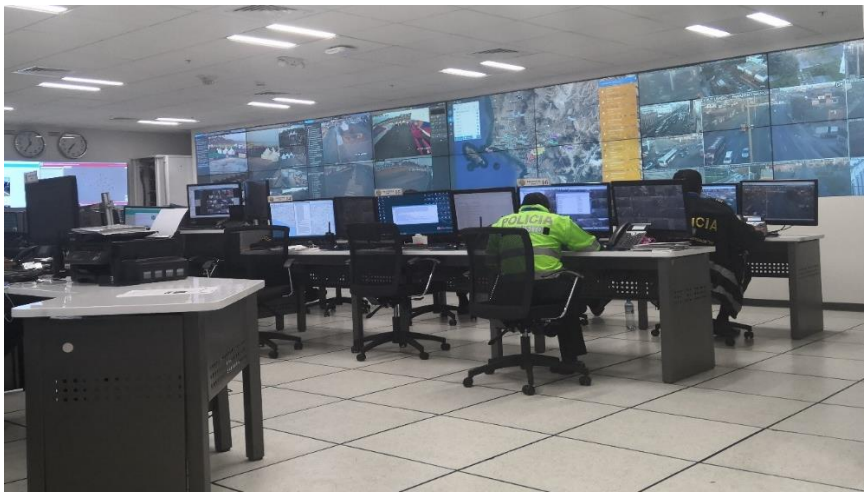


Figura 20. Prueba de validación del funcionamiento del sistema del mural de video

Fuente: Autoría propia

Procedemos a validar el funcionamiento del sistema genetec security center, en la Figura 21 nos muestra el funcionamiento de la plataforma de video genetec, el cual está diseñado para la administración de las cámaras de las diferentes sedes de forma remota a través del diseño de arquitectura de federación, en la imagen se muestra como prueba la visualización de 4 cámaras de la sede estadio nacional.

Figura 21. Prueba de validación del funcionamiento de la plataforma de video genetec.

Fuente: Autoría propia

3.1.7. Análisis de incidentes

Como último y sesto paso procedemos a realizar el desarrollo del análisis de incidentes, para este análisis se tomó como antecedente el evento deportivo Juegos Bolivarianos 2013 celebrado en el Perú. Se procede a realizar un análisis comparativo y cuantitativo en proporción a los asistentes de ambos eventos, "En los Juegos Deportivos Bolivarianos Trujillo 2013 se registraron un promedio de 38 mil asistentes y se detectaron un promedio de 63 incidentes contra la seguridad pública durante el desarrollo del evento" (Operador de videovigilancia, 2019), Estos datos nos darán el siguiente resultado:

$$\frac{\text{Número de incidentes X 100}}{\text{Número de asistentes}} = \text{Resultado en porcentaje}$$

$$\frac{63 \times 100}{38\,000} = 0.16\%$$

Este resultado del 0.16% es el porcentaje de incidencia respecto a la cantidad de asistentes y nos es útil para el análisis comparativo. "En los Juegos Panamericanos

Lima 2019 se registró un promedio de 170 314 y se detectaron un promedio de 158 incidentes contra la seguridad pública durante el desarrollo del evento" (Operador de videovigilancia, 2019). Estos datos nos darán el siguiente resultado:

$$\frac{158 \times 100}{170314} = 0.09\%$$

Este resultado del 0.09% es el porcentaje de incidencia respecto a la cantidad de asistentes y nos es útil para el análisis comparativo. En la Figura 22 se muestra la comparación de los resultados.

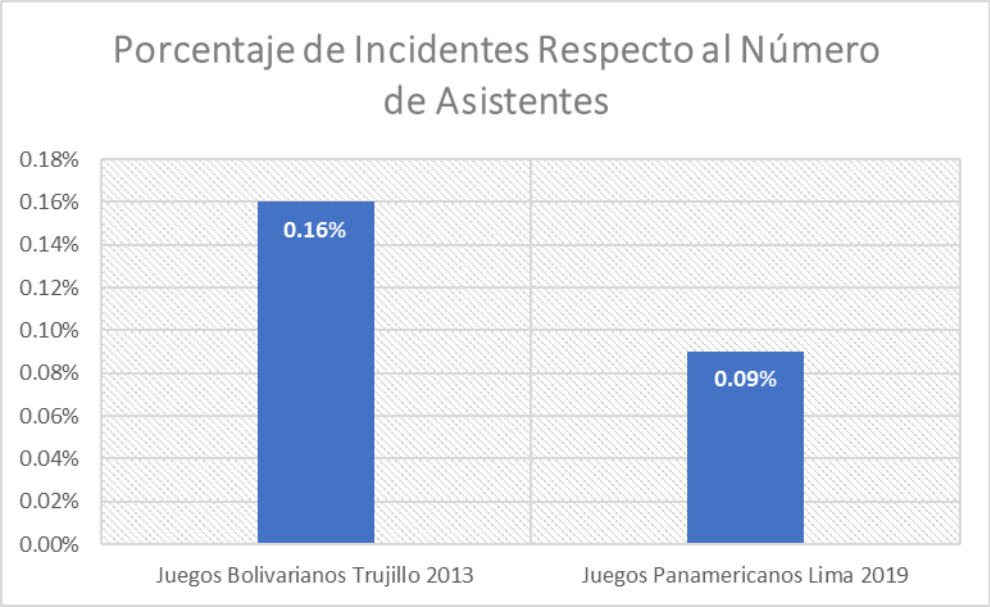


Figura 22. Porcentaje de incidentes respecto al número de asistentes

Fuente: Autoría propia

Como se observa en la Figura 22 se evidencia una reducción de los incidentes de un 0.7% respecto a la cantidad de asistentes.

Los factores que determinaron la reducción de incidente fue una mejor preparación a través de organismos públicos y privados juntamente con la implementación de nueva tecnología en vigilancia, prevención y despliegue de personal de seguridad tanto privado como estatal. En los juegos Deportivos

Bolivarianos Trujillo 2013 no se contaba con un centro de operaciones de seguridad, solo se contaba con soluciones de CCTV internas de cada sede las cuales no estaban integradas como un sistema global, además estas sedes contaban con un número menor de cámaras, el trabajo de seguridad se llevó principalmente por personas las cuales tenían comunicación vía radio o celular. Al no tener una central principal como centro de operaciones dificulta el mando y control, afectando la prevención y el tiempo de respuesta sobre los incidentes. Si bien es cierto que se pudo controlar de manera efectiva teniendo un número reducido de incidentes, este hecho se ayudó del número de asistentes tanto de deportistas como no deportistas y la ubicación de la sede en la ciudad de Trujillo teniendo un número reducido de habitantes a comparación de la capital Lima. En los Juegos Panamericanos Lima 2019 se implementó un centro de operaciones de seguridad, ayudando así al sistema de mando y control para la prevención y accionar de incidentes, teniendo un tiempo de respuesta más corto gracias a la tecnología implementada de video vigilancia y al personal especializado de seguridad tanto privado como estatal. El centro de control tiene la capacidad de integrar todas las sedes deportivas, convirtiendo a si en una solución globalizada, pero respetando la autonomía de cada sede. Además, se incrementó el número de cámaras en cada sede para salvaguardar la seguridad de los participantes deportistas y no deportistas. El resultado fue favorable tomando como base el evento deportivo anterior y la gran acogida que tuvo por parte del público en general superando en un 77.69% de participantes al evento anterior.

CAPÍTULO IV
RESULTADOS

4.1. Resultados

En este capítulo desarrollaremos los resultados en conjunto del centro de operaciones de seguridad.

- Solicitud de video de video a demanda, el uso de la arquitectura federation de genetec permite monitorear sititos remotos independientes como si fueran parte de un solo sistema virtual. Al ser una arquitectura federada la visualización de las cámaras de un sitio remoto a la central es a demanda, es decir podemos controlar el ancho de banda que transmite desde una sede remota a la central y limitarla a lo disponible (no transmite siempre, solo cuando el operador lo solicite). Este beneficio de poder controlar el flujo de video ayuda a la red a no saturarse o trabajar en sus límites. Ejemplo: ocurrió un accidente de tránsito en los alrededores de la sede polideportivo Callao, el comandante de la PNP ordeno a los operadores identificar los daños causados, para una mejor revisión los operadores deciden incrementar los fps del streaming de video de las cámaras localizadas en el lugar de accidente, el streaming estándar es de 15 fps y lo suben a 30 fps. El ancho de banda de la central está diseñado para soportar 761 cámaras a una transmisión de 2 mbps, pero la arquitectura federada no usa el 100% del ancho de banda solo un porcentaje de las cámaras monitoreadas en tiempo real. Así cuando incrementan el streaming a 30 fps también incrementan la trasmisión a 4 mbps por cámara, al incrementar la transmisión no se satura la red y tampoco afecta a los otros streaming de video de los demás operadores.

- Reducción del cuello de botella, otro de los beneficios de la arquitectura federation es la no necesidad de trasladar todo el flujo de video de las 761 cámaras de las 15 sedes deportivas al centro de operaciones de seguridad, aparte de acceder al video bajo demanda se optimiza el uso del ancho de banda y se evita el fenómeno llamado cuello de botella.
- No existe perdida de video o datos por problemas de red, la grabación de video es de manera local y por un breve periodo de 7 días. Al ser un sistema independiente del centro de operaciones de seguridad, asegura no perder los datos de la grabación por problemas de red (intermitencia de la red, perdida de red por factores externos, etc.) entre las sedes y la central. Ejemplo: la sede Punta Roca perdió conexión con el centro de operaciones de seguridad el día 5 de agosto a las 3:00 a.m. por el tiempo de 2 horas, los problemas se debieron a pruebas del proveedor de la red con el ancho de banda. Al retomar la comunicación con la sede Punta Roca se procedió a verificar si hubo perdida de grabación y tal como se muestra en la *Figura 23* no existió perdida de grabación teniendo un registro continuo sin interrupción.

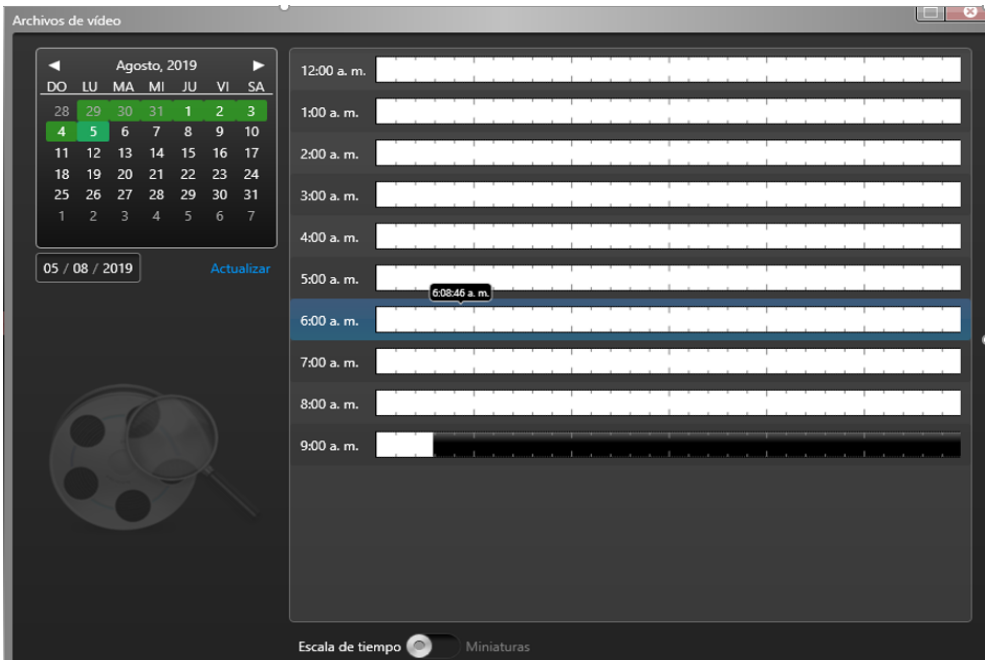


Figura 23. Tiempo de grabación sin registros de interrupción.

Fuente: Autoría propia

- Administración de usuarios, la plataforma de video genetec integra el active directory esto permite centralizar la entrada de usuarios, administra a los usuarios otorgando cuentas con distintos privilegios, es decir selecciona que usuarios pueden administrar o visualizar las cámaras remotamente, también puede denegar el acceso a grupos de cámaras a usuarios específicos o viceversa.
- La administración de alarmas y generación de reportes son centralizan en el centro de operaciones de seguridad, es decir cada vez que exista un problema en el sistema (cámara desconectada, intermitencia de red, etc.), genetec a través de su plataforma de gestión de video vigilancia manda una alerta a los operadores para que puedan estar al tanto y resolver el problema.
- Celulares usados como cámaras móviles, la plataforma de video vigilancia integra el nuevo servicio de Mobile, el cual proporciona acceso desde dispositivos IOS y Android. Esto quiere decir que el personal del cliente puede transmitir desde su celular en lugares donde no exista visión de las cámaras de seguridad y la información grabada se almacena en los servidores del centro de operaciones de seguridad. El servicio Mobile usa la resolución de la transmisión remota de las cámaras como fueron configuradas en security center y el tras codifica en resoluciones de teléfonos móviles (320x240), el máximo número de conexiones móviles es de 50 usuarios.
- Reducción de incidentes contra la seguridad durante el progreso de los juegos panamericanos Lima 2019, para el análisis del resultado se tomó como antecedente el evento deportivo Juegos bolivarianos Trujillo 2013 celebrado en el Perú. Se realizó un análisis comparativo cuantitativo en proporción a los asistentes de ambos eventos, el resultado fue una reducción de los incidentes de un 0.7% respecto a la cantidad de asistentes.

4.1.1. Análisis comparativo de los software y hardware utilizados

En concordancia con los softwares actuales se observa una nueva integración que muestra un enfoque completo para la seguridad y la vigilancia bajo la interfaz del software Genetec, donde se observó que los operadores del sistema pueden visualizar y controlar de forma remota los diseños de mosaicos y el contenido decodificado por Mura IPX en las paredes de video a través de funciones simples de arrastrar y soltar, bajo este precepto se puedo encontrar que mediante esta plataforma los operadores tienen control total sobre las transmisiones de video en la pared de video, ya sea que necesiten mostrar secuencias de cámaras de video en vivo o reproducir transmisiones desde un servidor de video.

Además del contenido de video, así también se pudo encontrar que el complemento también puede administrar contenido que no es de video, como mapas, páginas web y datos de control, que se pueden mostrar en la pared controlando todas las fuentes y ajustes preestablecidos, lo que proporciona un completo de extremo a extremo. solución en red.

Respecto a Matrox video también se puede mencionar que se encontró que tiende a ser una plataforma versátil ya que contiene una cartera completa del mejor hardware, software, API y SDK de su clase, así también se puede mencionar que Matrox Video permite a los OEM, integradores de sistemas, socios de canal de valor agregado y usuarios finales superar los límites de la innovación en video.

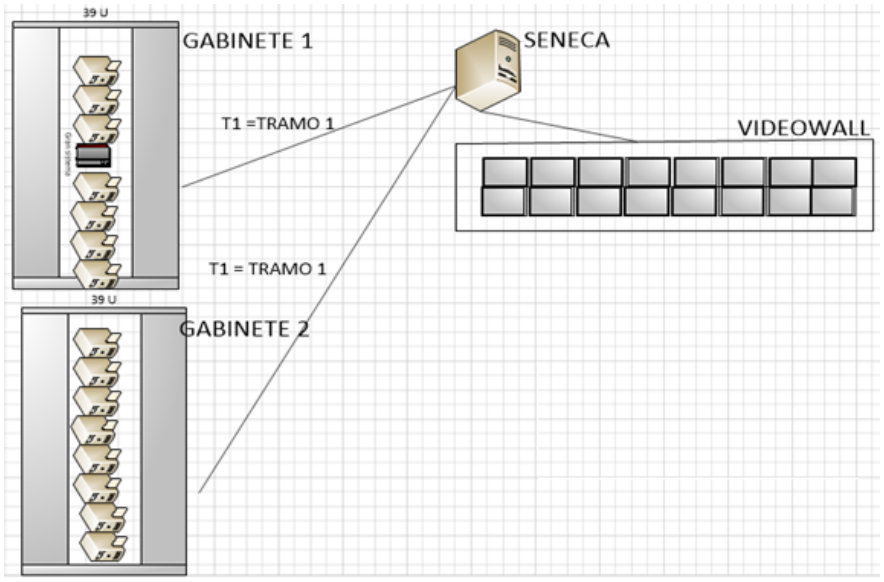
4.1.1.1. Hardware ATEN

El Sistema de control de hardware de ATEN se adapta perfectamente a todas las salas con múltiples dispositivos de hardware que necesiten de un control integrado. Gracias a una interfaz personalizable, con controles digitales o físicos, podrás crear tu propia configuración o utilizar la predeterminada.

No importan las dimensiones de la sala ni lo complicado que sea el hardware, el Sistema de control de ATEN se puede implementar en 3 sencillos pasos: conectar los equipos de TI y el hardware audiovisual a un dispositivo central (controlador VK2100), configurar los perfiles y los ajustes de administración (software VK6000) y, por último, disfrutar del control más fácil de utilizar.

Dentro de los beneficios que presenta es: facilidad para las conferencias y colaboración, salas de control, y lograr una buena distribución multimedia.

La siguiente figura representa gráficamente la conexión de cada CPU de los usuarios ubicado en el gabinete y su conexión con el controlador Seneca, asimismo se detalla la conexión de los 16 monitores (Videowall) hacia el controlador Seneca.



a. Conexiones estándar

Podrás conectar y controlar los dispositivos de hardware más utilizados del mercado gracias a los puertos Ethernet, serie, E/S, relé e infrarrojos.

b. Firmware compatible

La biblioteca de controladores del software VK6000 está equipada con los controladores de más de 10 000 dispositivos.

Podrás añadir el controlador que necesites, con lo que te permite utilizar innumerables dispositivos.

c. Facilidad de ampliación

Para poder controlar todavía más dispositivos con puertos serie, de retransmisión o infrarrojos, los usuarios pueden recurrir a los módulos de expansión.

Los módulos de expansión se pueden conectar al VK2100 desde la ubicación que desee ya que disponen de una conexión basada en Ethernet.

d. Control simplificado

Un controlador de hardware centraliza, automatiza e integra el control de los diferentes dispositivos de hardware. Permite crear perfiles y programar dispositivos para cambiar con rapidez una configuración o ahorrar energía

e. Interfaz del usuario personalizada

Botones físicos, sensores o una aplicación totalmente personalizada. Diseña tu interfaz de usuario a medida para utilizarla en varias plataformas. Con el sistema de aplicaciones “arrastrar y colocar” la programación es opcional.

4.1.1.2. Hardware ATEN

Continuamente, las características principales de los productos y soluciones, es la adquisición de nuevas tecnologías. SENECA es integrante principal de la misión empresarial, la de asegurar todo el periodo de tratamiento de la señal - alimentación y aislamiento galvánico incluidos hasta la entrega de la información.

El Extensor de KVM usa una conexión a través de IP, compuesta por un equipo de transmisión que esta conecto al computador, y un equipo de recepción que autoriza el acceso a la consola desde un lugar remoto.

Para la conexión del computador se ejecuta desde la consola remota el cual tiene una conexión TCP/IP conectado a través de un cable UTP Cat6 que permite la administración de multipunto a multipunto, de punto a multipunto y punto a punto.

Por "Obtención de información" se entiende la adquisición automática de información (ejemplos: presiones, capacidades, niveles de energía, recuentos), que, por lo común, proveen los sensores, transductores y analizadores a fin de dar seguimiento a los instrumentos, equipos, variables y parámetros también desde lugares remotos a través de un canal de transmisión de datos serial, fieldbus, Ethernet, fibra óptica, radio).

Por el lado del hardware SENECA propone módulos I/O puntos aislados o integrados en CPU de altas consideraciones (entradas analógicas, digitales de sensores (TC, RTD, celdas de carga) y analizadores de red monofásica o trifásica; interfaz RS485 Modbus RTU, hasta 1.200 m o CANopen).

Los módulos I/O de la Serie Z-PC consiguen información a través del uso de cuadros, sub-cuadros e instalaciones de diferentes tipos: panales de mando, cuadros de automatización locales o remotos, módulo individual, kit portátil o de banco, etc.

Por el lado del software SENECA ofrece software y herramientas PC Windows como DATA RECORDER, driver NI LabView, tecnologías OPC, Librería Microsoft Visual Estudio y Web Editor.

Así también se muestra los siguientes cuadros comparativos advertidos en este estudio.

Tabla 11. *Hardware ATEN y SENECA*

ATEN	**SENECA**

-Calidad de vídeo – hasta 1920 x 1200 a 60 Hz; 24 bits de profundidad de color -Conexiones flexibles - permite varias conexiones de extensores y matrices para instalaciones de multipantalla y aplicaciones de pared de vídeo -Admite salida de vídeo digital y analógica con 2 salidas de vídeo como canal independiente -Inserción y extracción - comparta contenido al instante con solo un clic	-Procesador Intel® Core ™ i7 de 8.a generación -Hasta 8 salidas 4K de alta densidad -Hasta 9 salidas HD de alta densidad -Opciones de GPU de altura completa y ancho completo -Capacidad 4K -Factor de forma de 1U de profundidad corta

Fuente: Autoría Propia

4.1.2. Normativa sobre la operatividad

Así también se brinda un análisis de los puntos clave en la normativa respecto a las características técnicas y de interoperabilidad de los sistemas de video vigilancia

Las características mínimas exigidas de las cámaras:

a. Video.

- El dispositivo de la cámara debe contar con tecnología Digital IP.
- El dispositivo de la cámara debe contar con una resolución mínima de 1.3 MP.
- La cámara cuenta con un lente el cual debe ser Varifocal: 4.3 mm a 129 mm. F1.6 (hasta el cierre) a F4.7 (hasta el cierre).
- El sensor de la cámara a implementar debe ser CCD 1/3'' o CMOS opcional.
- El zoom de la cámara debe ser mínimo de 30X óptico (4.3 mm).
- La cámara debe trabajar como mínimo a 30 fps.

- La cámara debe trabajar a una compresión de H.265.
- La cámara instalada debe ejecutar ajuste de imagen en balance de blancos, compensación de contraluz (auto-iris), nitidez, brillo y color.
- La cámara deberá tener incluida la tecnología Día/Noche.
- Video inteligente: se refiere a la detección de movimiento por video (depende del sistema).
- La alarma debe ser activado por el video inteligente.

b. Nivel de Red

- La cámara IP es compatible con los diferentes protocolos de comunicación los cuales son: RMON, DVMRP, SSHv2, Syslog, PIM-SM, SNMP v2c/v3, DHCP, RIPv2/OSPF, IGMP, HTTPS, QoS DSCP, SNTP, IPv4/v6, FTP, TFTP.
- La seguridad debe concebir el uso de clave, filtro de dirección IP, cifrado HTTPS, control de acceso a red IEEE 802.1x.
- La cámara debe tener un sistema escalable para albergar a nuevas versiones tecnológicas, subir archivos por medio de correo electrónico y FTP.

c. Nivel Físico

- La cámara a emplear por los SVV del país debe ser del tipo PTZ y/o domo PTZ.
- La cámara PTZ deberá conceder movimiento vertical de 0° a 90° y movimiento horizontal de 360°.
- La cámara debe contar con protección contra aspectos climatológicos y vandalismo. Debe contar con tecnología IP66.
- La cámara debe contar con el soporte correcto para su instalación.

- La cámara debe contar con un peso menor a 10 Kg.
- La cámara debe soportar el intervalo de temperatura entre –35°C a 60 °C.
- La cámara debe contar con conexión de entrada compatibles con los conectores RJ45 10BASE-T/100BASE-TX.
- La cámara debe ser compatible con PoE+.

De igual forma se brinda un análisis de los lineamientos normativos respecto a los objetivos de un sistema de video vigilancia, teniendo en consideración los valores mínimos que debe cumplir para ser implementado.

- Dar un seguimiento a vehículos.
- Observar cruceros.
- Observar salidas y entradas de las ciudades.
- Observar concentraciones públicas recreativas y comerciales.
- Observar lugares de alta potencialidad delictiva.
- Ayuda en eventos de protección civil.
- Ayuda constante a la administración municipal.
- La constante observación de salidas y entradas de lugares delictivos.
- Observar y cuidar instituciones de educación medio y superior.
- Observar lugares de pasos fronterizos y concurrencia turísticas.
- Los sistemas de video vigilancia privados externos deben ser integrados.
- Observar y cuidara la población infantil en Instituciones educativas iniciales.
- Observar y cuidara la actividad económica productiva.

- Observar y guardar el patrimonio público y privado.

4.2. Presupuesto

El proyecto tiene una estimación aproximada de 226,560.00 dólares americanos, las cuales se describen en la Tabla 12.

Tabla 12. *Solución para Centro de operaciones de seguridad*

SOLUCION PARA CENTRO DE OPEREACIONES DE SEGURIDAD							
Item	Marca	Modelo	Descripción	Unidad de medida	Cantidad	Precio Unitario ($)	Precio Total ($)
1. Estaciones de trabajo							
1.1	ATEN	KE6940	DVI Dual Display KVM Over IP Extender	Unid	16	$ 2,500.00	$ 40,000.00
1.2	KOPUL	S/N	DVI-D Cable	Unid	32	$ 8.00	$ 256.00
1.3	KRAMER	S/N	Four Pair STP Data Cable	Unid	16	$ 250.00	$ 4,000.00
2. Equipos Videowall							
2.1	SENECA	VWC-MURA	Servidor Seneca para videowall	Unid	1	$ 40,000.00	$ 40,000.00
2.2	S/N	S/N	Accesorios de instalación: -Canaletas para cable de video -Cable de energía -Cable HDMI 15 Mts Promedio -Peinado y ordenamiento de -Cable de Poder para monitores. -Drywall, parantes, masillas, pintura, abiquería. -Caja de pase, faceplate y conectores de video HDMII.	Glb	1	$ 2,000.00	$ 2,000.00
3. Software Videwall							
3.1	MATROX	6.4	Matrox MuraControl	Unid	1	$ 5,000.00	$ 5,000.00
4. Plataforma de video							
4.1	GENETEC	GSC-BASE-5.7	Genetec Security Center (GSC) Versión 5.7	Unid	1	$120,000.00	$ 120,000.00
5. Servicios							
5.1			Servicios de Instalación y configuración	Glb.	1	$ 20,000.00	$ 20,000.00
6. Gatos Generales							
6.1			Gastos Generales Imprevistos	Glb.	1	$ 5,000.00	$ 5,000.00
						Sub Total	$ 192,000.00
						IGV (18%)	$ 34,560.00
						Total	$ 226,560.00

Fuente: Autoría propia

CONCLUSIONES

- Concluimos que, el diseño e implementación de un centro de operaciones de seguridad para el evento deportivo Juegos Panamericanos Lima 2019, se encontró un ambiente adecuado, ya que se permitió mediante el software y hardware instalado tener mayor certeza respecto a la seguridad tanto de las personas asistentes como de los deportistas, disminuyendo de manera significativa las ocurrencias imprevistas, ello por el sistema de seguridad. Siendo así, el Controlador de pantalla de vídeo de Séneca fue la mejor alternativa de solución Matrox certificada, porque que fue diseñada para alojar hasta 4 tarjetas MURA, porque cuenta con un sistema de procesador Intel® Core ™ i7, el que puede abastecer y lograr un rendimiento excepcional.

- Ciertamente, el proceso de implementación de módulos de monitorio a través de consolas KVM sobre IP, mejoro de manera sustancial la distribución en la sala del centro de comando de seguridad la cual evidencio una mejoría en el resguardo de los ordenadores en un lugar con un ambiente optimo (data center). Tomando en cuenta que el controlador de Videowall certificado Matrox está construido en un chasis exclusivo para proporcionar una refrigeración adecuada para una configuración óptima, por lo que estos módulos dieron lugar a un ambiente favorable para la actividad de los operadores que administran y controlan de forma remota las 761 cámaras de las 15 sedes deportivas, a través de la arquitectura de federation de Genetec. A través de este sistema basado en servicios de red se logró manejar diferentes de ocurrencias con diferentes tipos de componentes; porque la conexión de cada CPU de los usuarios ubicado en el gabinete y su conexión con el controlador Seneca permitió tener mayor alcance.

- Arrojamos, que el diseño e implementación del sistema de video vigilancia a través de la plataforma Genetec, mostró de manera eficiente su capacidad para integrar las plataformas de video independientes de las 15 sedes deportivas así también se observó que al margen de la capacidad de integración mantuvo conservado su independencia, así mismo se integró un total de 761 cámaras, las cuales provenían de diferentes marcas y modelos; lo observado demostró la capacidad de la plataforma Genetec para desarrollar un sistema que tuvo carácter global de las cámaras inmersas en dicho evento deportivo creando un núcleo globalizado de cámaras video vigilancia remota. Este resultado se debe a que el hardware elegido cuenta con soporte para hasta 16 salidas de Full HD en un sistema de 4 tarjetas, el VWC-4 tiene opciones adicionales para alimentación redundante.

- Finalmente, se advierte que la combinación de la decodificación de alta densidad en la pared de video y el fácil control desde la interfaz del centro de seguridad realmente genera una simplificación de los operadores de Genetec, mientras mejora significativamente el proceso de toma de decisiones; asimismo, los resultados obtenidos muestran que se logró medir las incidencias de posibles acciones de riesgo a la seguridad de los deportistas y expectantes, quienes se identificaron con los indicadores clave de rendimiento (KPI), en cada evento deportivo se logró medir exitosamente el porcentaje de incidencias respecto a la cantidad de asistentes, donde se puso en manifiesto un resultado final, donde se pudo reducir los incidentes al 0.7%. Es decir, se logró una reducción de incidentes a comparación del evento anterior, porque el controlador SENECA permitió la división de 8 puertos tipo KX20, cada KX20 tiene en un extremo un conector y por otro extremo 4 conectores DVI cada uno con su respectivo adaptador DVI a HDMI. Es decir, en total se utilizó 32 convertidores de DVI a HDMI y 8 cables tipo pulpo de 4 salidas DVI para el Seneca que tiene como función transmitir imágenes de los monitores de los operadores al Videowall.

RECOMENDACIONES

- A los organizadores que se desarrolle lineamiento para mejorar el COS, con el objeto de evitar la saturación del COS en el día, considerando factores como el apoyo desde un enfoque ambiental agradable que no cause incomodidad o déficit de atención.
- A los Organizadores desarrollar conjunto de capacitaciones dirigidos a los operadores en el manejo del cliente Genetec para un mejor uso de la plataforma de video vigilancia y así poder explotar todas sus funcionalidades integradas.
- A los ingenieros residentes, que realicen jornadas de reconocimiento de la infraestructura interna y externa del centro de operaciones de seguridad para la solución a los incidentes tiempos relativamente cortos, de igual forma se insta al uso de instrumentos portátiles de gama alta o media para mejorar el nivel de respuesta.
- A los Organizadores, que implementen directrices para potenciar la capacidad del sistema de seguridad y mermar las incidencias negativas brindando iluminación adecuada, evitando de esta forma efectos negativos de la iluminación por la especial foto sensibilidad de los monitores de ordenador y las pantallas de monitorización lo que genera perjuicios en el óptimo desarrollo de las actividades del Centro de Operaciones de Seguridad.

GLOSARIO

- **Ancho de banda:** Es la cantidad de información que se puede enviar a través de una conexión de red en un período de tiempo. El ancho de banda se mide generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps)
- **Bps:** bits por segundo, es la unidad de medida de transferencia de información **Ordenador**: Máquina electrónica capaz de almacenar información y tratarla automáticamente mediante operaciones matemáticas y lógicas controladas por programas informáticos.
- **Consola:** Aparato electrónico que se conecta a un monitor.
- **DVI:** Digital Visual Interface es un cable que trasporta video en alta calidad.
- **FPS:** es la velocidad en el que se muestra una frecuencia de fotogramas.
- **H264:** es un formato de compresión de video.
- **H265:** es un formato de compresión de video, sucesor del H264.
- **Hardware:** es toda parte física de una computadora o bien de un sistema informático
- **HDMI:** High-Definition Multimedia Interface es un cable de video que trasporta video y multimedia, es superior al cable DVI.
- **Incidente**: un incidente es un suceso que ocurre en cualquier ubicación que puede, o no, ocasionar algún daño a la persona o personas.
- **Mural de video:** es una pared o muro con instalación existente de pantallas o monitores.
- **Servidor:** Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

- **Software** es el equipamiento lógico que poseen los sistemas informáticos como computadoras y otros aparatos como teléfonos inteligentes y diversos aparatos tecnológicos.
- **TB:** (Terabyte) Es una unidad de medida igual a 1.024GB. El terabyte se utiliza para cuantificar memoria o capacidad de disco. Ver definición de GB.
- **TCP/IP:** Protocolo de Control de Transmisión / Protocolo de Internet, es el protocolo de funcionamiento que se usa en las redes de equipos de transmisión para la correcta comunicación de todos los equipos.
- **Video a demanda:** es la visualización de un video solo cuando se requiere.
- **Video vigilancia:** es el monitoreo constate de un lugar o lugares, el objetivo depende de la institución u organismo.
- **Video Wall:** es una configuración especial de monitores o pantallas.

BIBLIOGRAFÍA

Arrow Electronics, Inc. (2018). *VWC-PLUS star guide*. Obtenido de https://www.senecadata.com/industry-solutions/video-wall-controllers/seneca-vwc-plus-video-wall-controller

ATEN International Co. Ltd. (2019). *KVM over IP matrix series: KVM over IP extender & CCKM KE matrix manager software user manual*. Obtenido de https://www.aten.com/la/es/products/kvm/extensores-kvm/ke6940ar/

Axis Comunicactions Corp. (2018). *Sistemas de gestión de video*. Obtenido de https://www.axis.com/es-pe/my-axis/newsletter

Buendía, R. (2016). *Diseño e implementación de un sistema completo de seguridad que contempla vídeo vigilancia móvil y posicionamiento global GPS en tiempo real, con monitoreo remoto para vehículos blindados de transporte de valores (Tesis de pregrado).* Ecuador: Universidad de las Fuerzas Armadas.

Camacho, E. (2017). *Análisis y diseño de un sistema de video vigilancia (CCTV) con fibra óptica aplicando la norma IEEE 802.3bm para el club internacional de Arequipa (tesis de pregrado).* Arequipa: Universidad Nacional de San Agustín de Arequipa.

Consultora Mercel . (2018). *Ranking mundial de calidad de vida (vigésimo).* New York: Mercer LLC.

Genetec Inc. . (2018). *https://www.genetec.com/es/soluciones/productos/security-center*. Obtenido de https://www.genetec.com/es/soluciones/productos/security-center

Genetec Inc. (2019). *Certificación de diseños de sistemas*. Obtenido de https://resources.genetec.com/books

Hammar, M. (2015). *ISO 9001 verificación de diseño vs validación de diseño*. Obtenido de https://advisera.com/9001academy/es/knowledgebase/iso-9001-verificacion-de-diseno-vs-validacion-de-diseno/

Instituto Militar de Estudios Superiores Escuela de Comando y Estado Mayor. (2006). *Los sistemas de comando y control*. Obtenido de http://www.imes.edu.uy/new/?page_id=2019

Lahoz, F. (2017). *Diseño de redes de cámaras inteligentes utilizando smartphones (tesis de pregrado)* . España: Universidad Autónoma de Madrid.

Lio, V. (28 de Diciembre de 2015). *Ciudades, cámaras de seguridad y video-vigilancia: estado del arte y perspectivas de investigación*. Obtenido de Conicet Digital: http//revistas.unc.edu.ar/index.php/astrolabio/article/view/9903

Martí, S. (2013). *Diseño de un sistema de televigilancia sobre IP para el edifico CRAI de la escuela politécnica superior de Gandía (tesis de pregrado).* España: Universidad Politécnica de Valencia, Valencia.

Matrox Graphics, Inc. (2017). *Matrox mura control for Windows user guide*. Obtenido de https://www.matrox.com/graphics/en/products/video-wall/muracontrol/

Ministerio do Esporte. (2013). *Memoria jogos pan-americanos.* Río de Janeiro: Gobierno Federal do Brasil.

Morales, C., Moreno, O., & Ortigoza, J. (2014). *Propuesta de un modelo de centro de operaciones de seguridad (soc) para fuerza aérea colombiana (tesis de pregrado).* Colombia: Universidad Piloto de Colombia.

Operador de videovigilancia. (11 de diciembre de 2019). comunicación personal.

Pérez, I. (2009). *Arquitectura de un sistema C4ISR para pequeñas unidades (tesis de doctoral).* España: Universidad Politécnica de Valencia, Valencia.

Regalado, O., Ayala, M., Chero, L., Yauri, Y., & Zevallos, A. (2015). *Juegos panamericanos Lima 2019: factores críticos para su organización.* . Lima: ESAN ediciones.

Salcedo, C. (2018). *Diseño de un centro de control y monitoreo (CCTV) con sistema de radioenlaces para la seguridad en la municipalidad de Islay Matarani (Tesis de pregrado).* . Arequipa: Universidad Nacional de San Agustín de Arequipa.

Salvador, P., Boronat, F., Montagud, M., & Marfil, D. (2017). Sistema videowall de bajo coste basado en raspberry pi, personalizable y configurable dinámica y remotamente vía web. Jitel 2017, 13(1), 317-318. Doi: https://dx.doi.org/10.4995/JITEL2017.2017.6. *Jitel*, https://dx.doi.org/10.4995/JITEL2017.2017.6.

Sierra, C. (2017). *Propuesta del Sistema de video vigilancia en la seguridad ciudadana distrito de Pueblo Libre 2016-2020 (tesis de maestría).* Lima: Universidad Cesar Vallejo.

Villa, H. (2015). *Un método para la definición de indicadores clave de rendimiento con base en objetivos de mejoramiento (tesis de maestría).* Colombia: Universidad Nacional de Colombia.

ANEXOS

Anexo 1. Imágenes de la instalación del servidor seneca.

Figura 24. Servidor seneca instalado

Fuente: Autoría propia.

Anexo 2. Imágenes de los ordenadores apilados en gabinetes

Figura 25. Gabinete con los ordenadores.

Fuente: Autoría propia.

Figura 26. Ordenador.

Fuente: Autoría propia.

Anexo 3. Imágenes de la instalación del cableado del servidor seneca

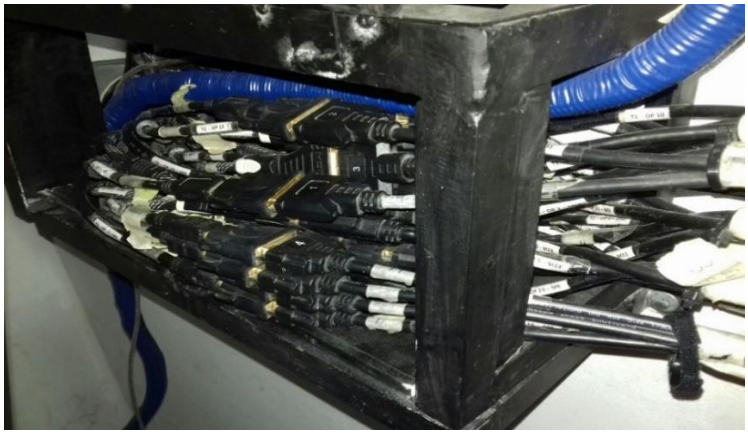


Figura 27. Cableado desde el servidor seneca.

Fuente: Autoría propia.

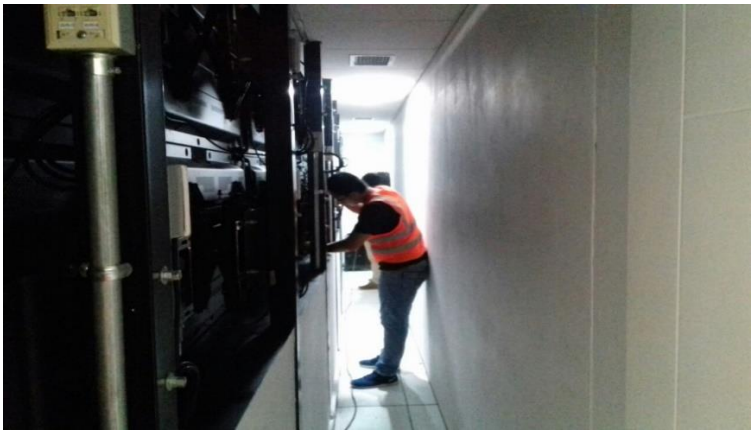


Figura 28. Instalación del cableado HDMI.

Fuente: Autoría propia.

Figura 29. Mural de video.

Fuente: Autoría propia.

Anexo 4. Imágenes de la instalación de los KVM.

Figura 30. KVM aten serie KE6940.

Fuente: Autoría propia.

Figura 31. Instalación del KVM en sus módulos.

Fuente: Autoría propia.

Anexo 5. Imágenes de la instalación del cableado de los KVM.

Figura 32. Ordenamiento del cableado del KVM

Fuente: Autoría propia.

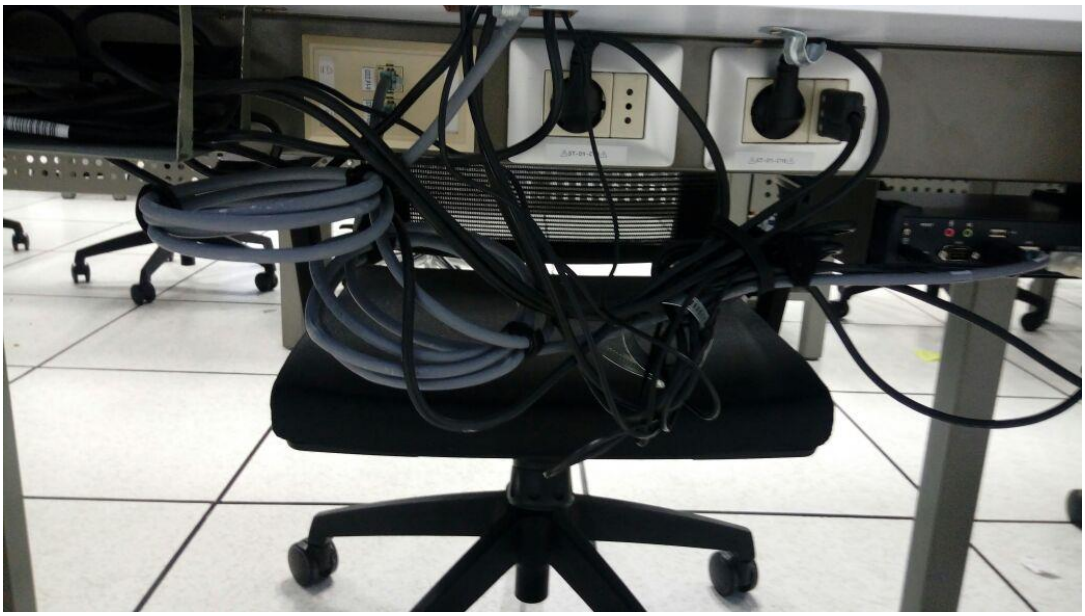


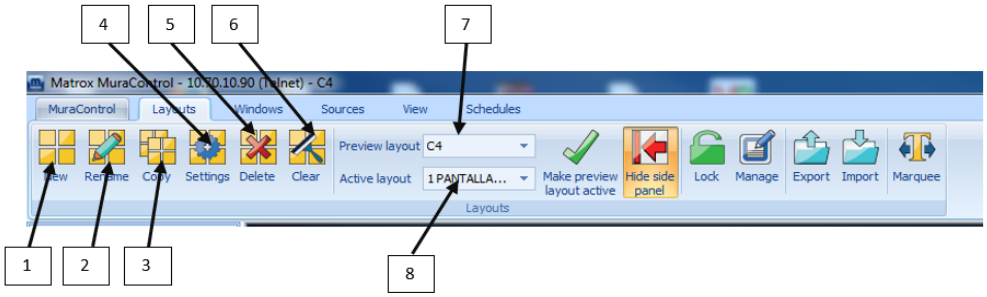
Figura 33. Cableado UTP Cat6A

Fuente: Autoría propia.

Anexo 6. Imágenes de la instalación del cableado de los KVM.

Figura 34. Icono del muracontrol.

Fuente: Autoría propia.



1- Crea los nuevos grupos de ventadas para poder guardar.
2- Cambio de nombre del grupo.
3- Copiar un grupo ya creado.
4- Ajustes de la ventana en su proyección.
5- Borra grupo seleccionado
6- Borrar en las ventanas del grupo creado.
7- Es una ventada preliminar para configurar sin muestran en el Videowall.
8- Es para mostrar la imagen el video Wall.

Figura 35. Barra de funciones del Software Muracontrol

Fuente: Autoría propia.

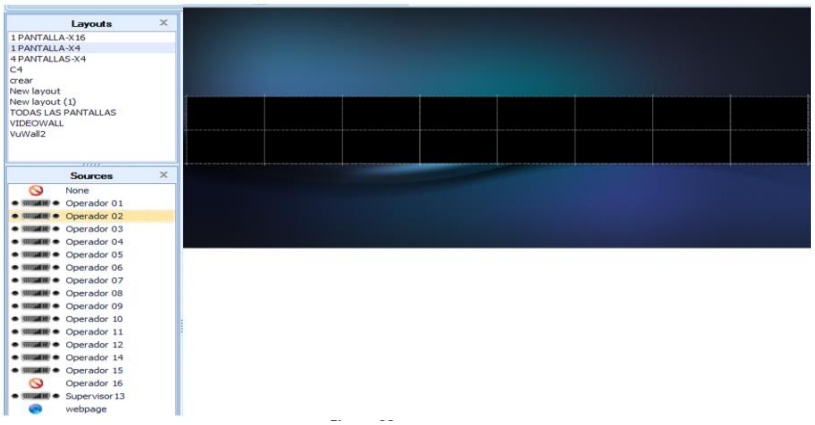


Figura 36. En la columna de la izquierda se muestra las estaciones de trabajo reconocidos por el Software Muracontrol.

Fuente: Autoría propia.

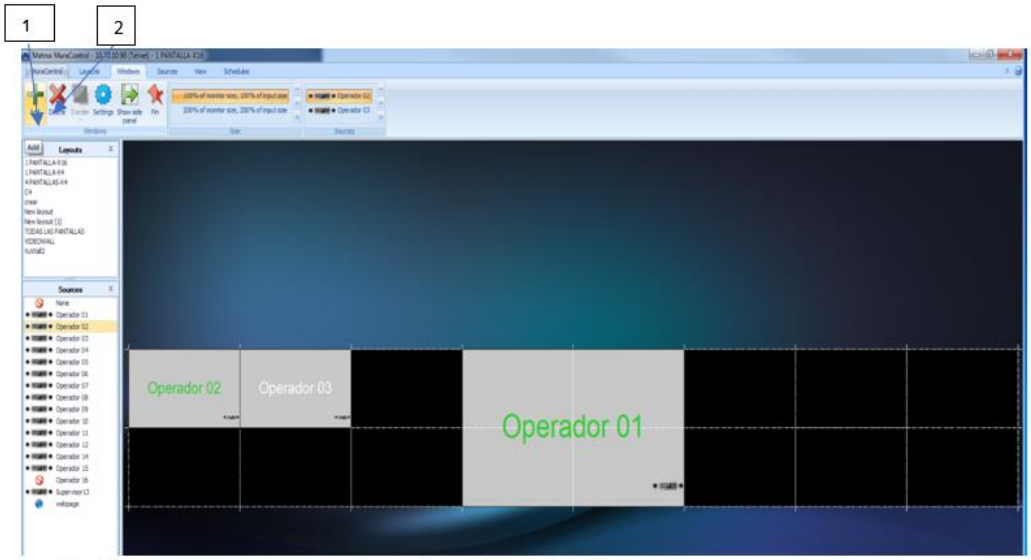


Figura 37. Seleccionamos la ventana de Windows para agregar a los operadores.

Fuente: Autoría propia.

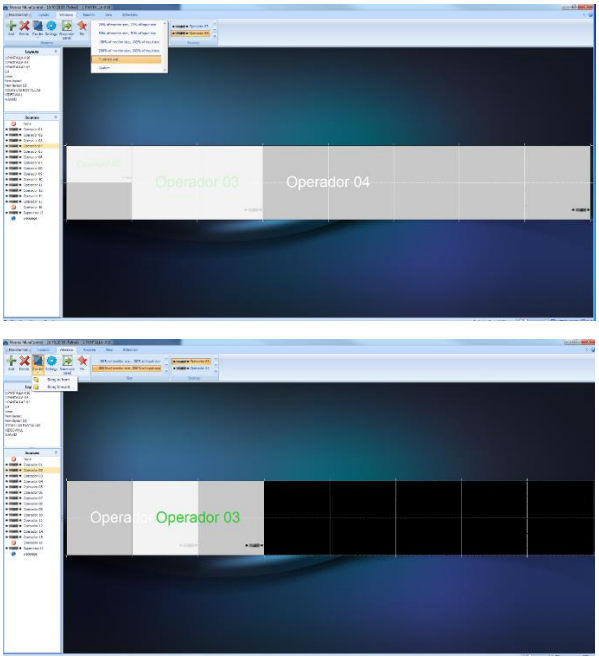


Figura 38. Procedimiento de asignación de pantalla.

Fuente: Autoría propia.

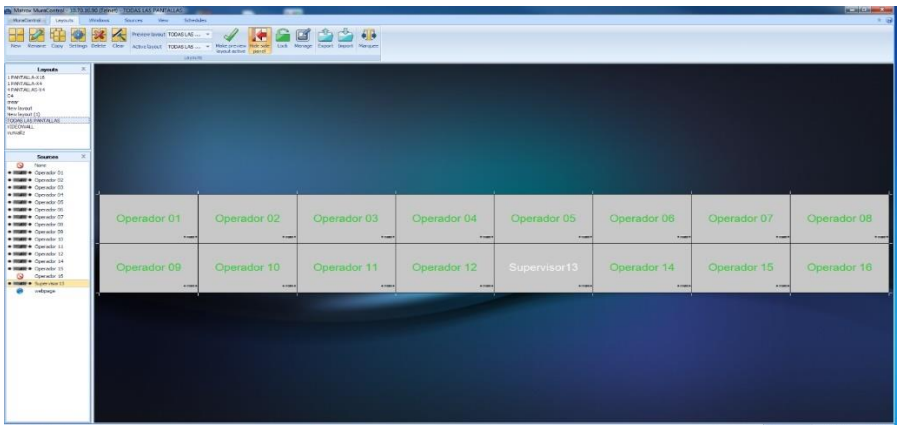


Figura 39. Plantilla armada para con cada uno de los operadores para que sus pantallas se visualicen en el videowall

Fuente: Autoría propia.

Anexo 7. Resultados de la configuración de genetec.

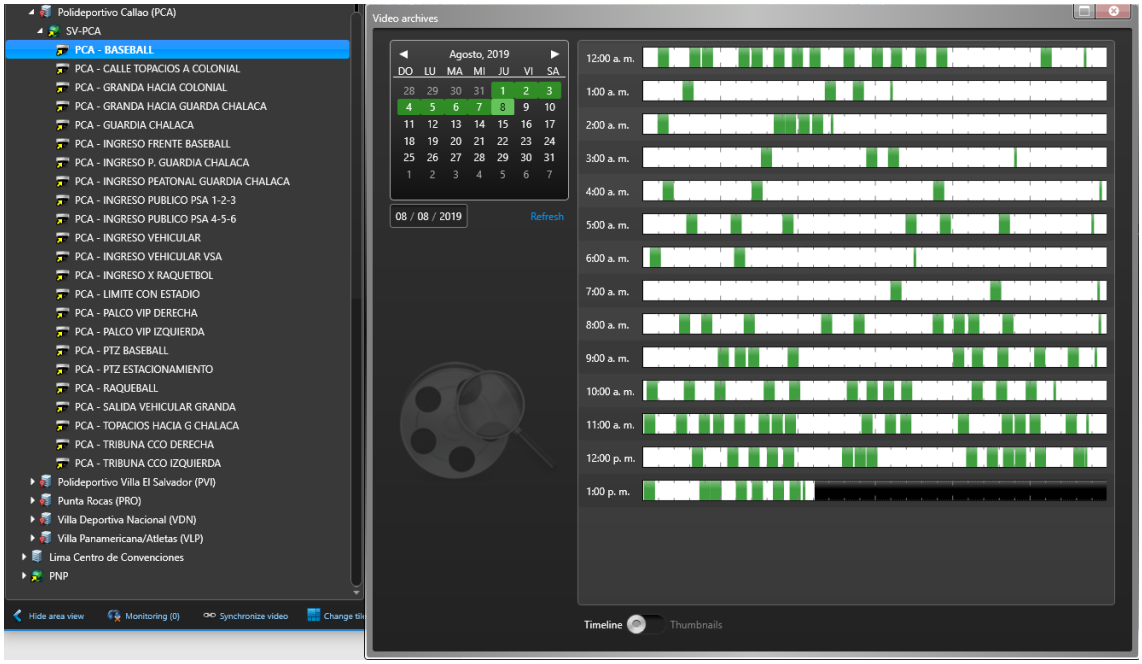


Figura 40. Sede – PCA (Polideportivo Villa regional del Callao).

Fuente: Autoría propia.

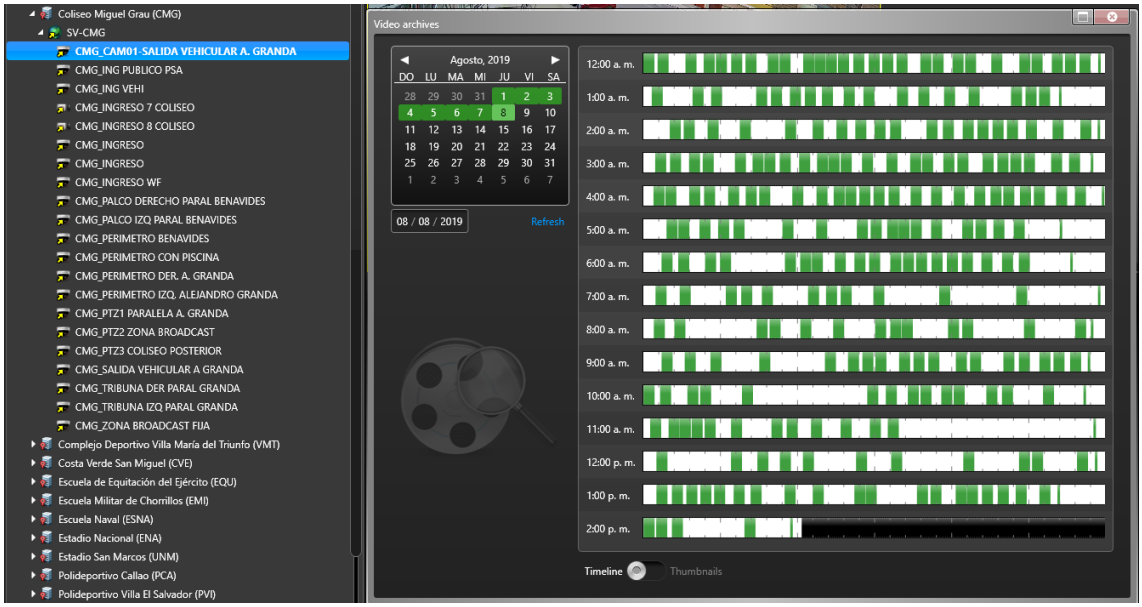


Figura 41. Sede – CMG (Coliseo Miguel Grau).

Fuente: Autoría propia.

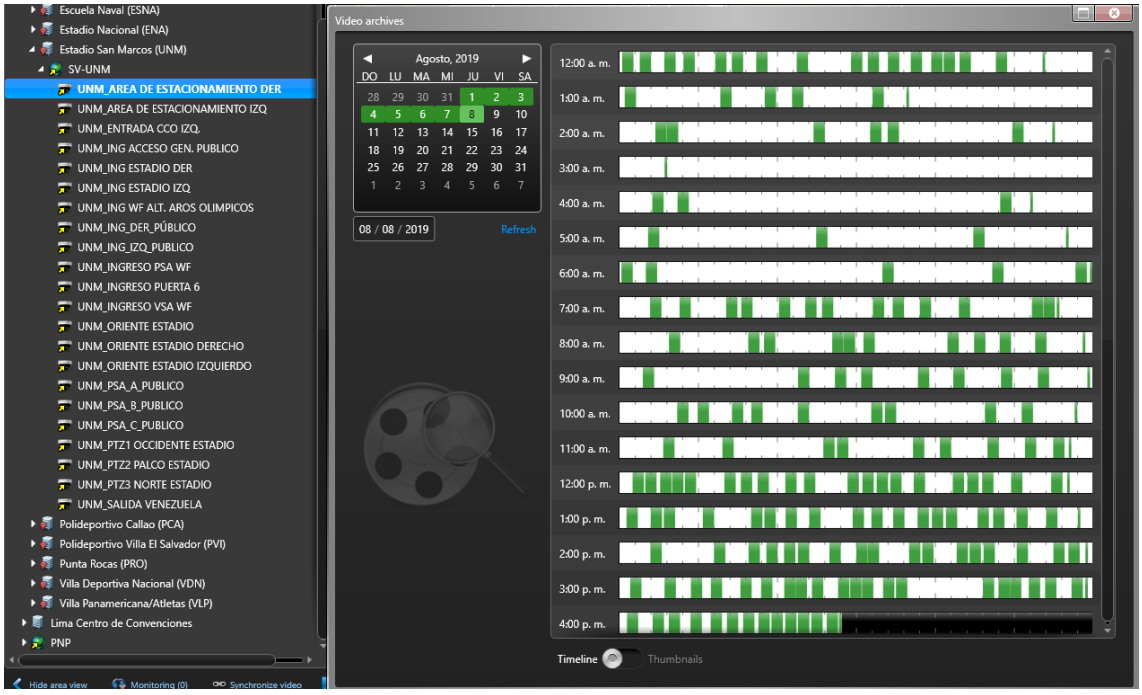


Figura 42. Sede – UNM (Estadio San Marcos).

Fuente: Autoría propia.

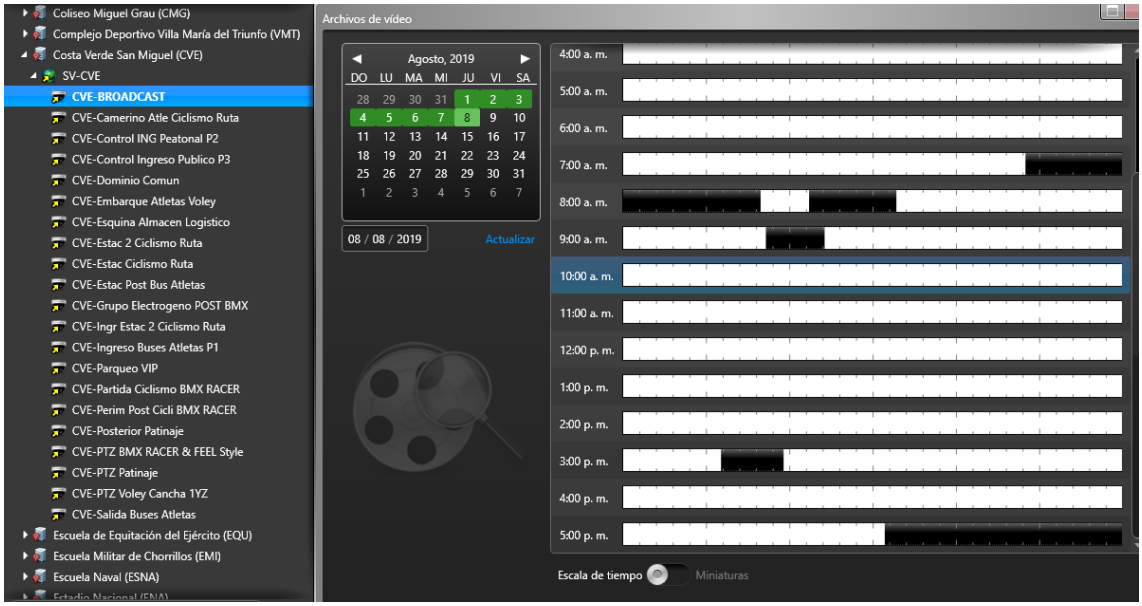


Figura 43. Sede – CVE (Costa Verde San Miguel).

Fuente: Autoría propia.

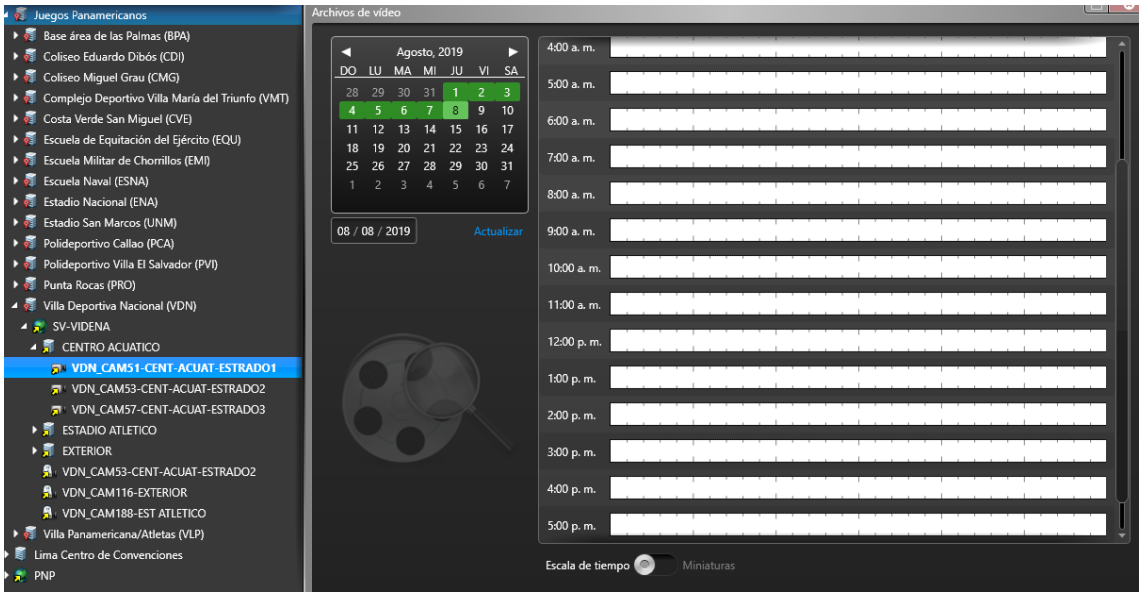


Figura 44. Sede – VDN (Villa Deportiva Nacional).

Fuente: Autoría propia.

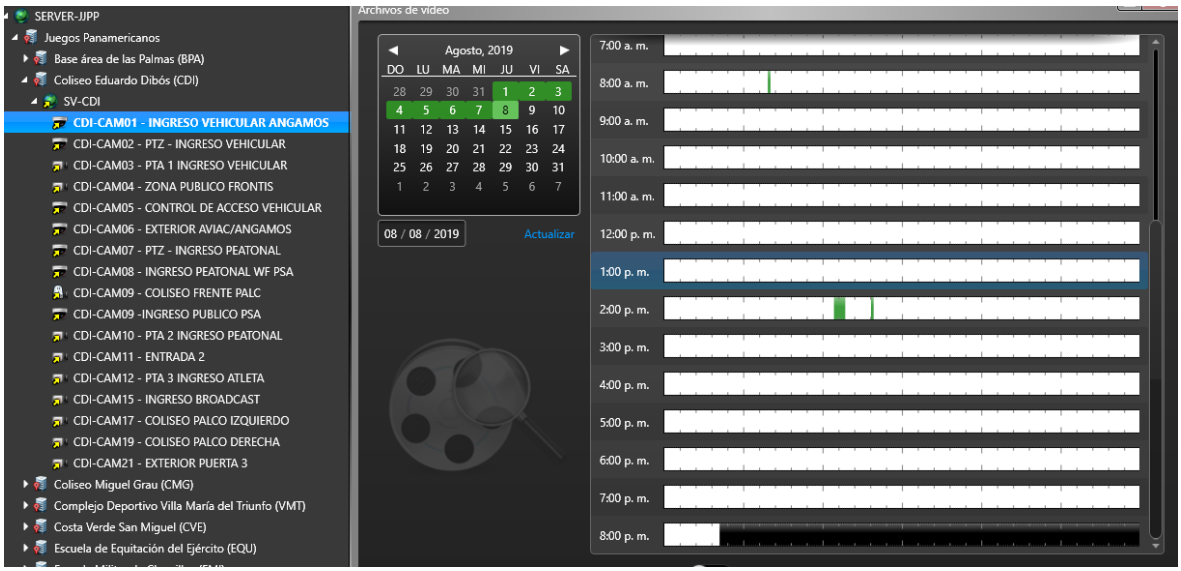


Figura 45. Sede – CDI (Coliseo Eduardo Dibós).

Fuente: Autoría propia.

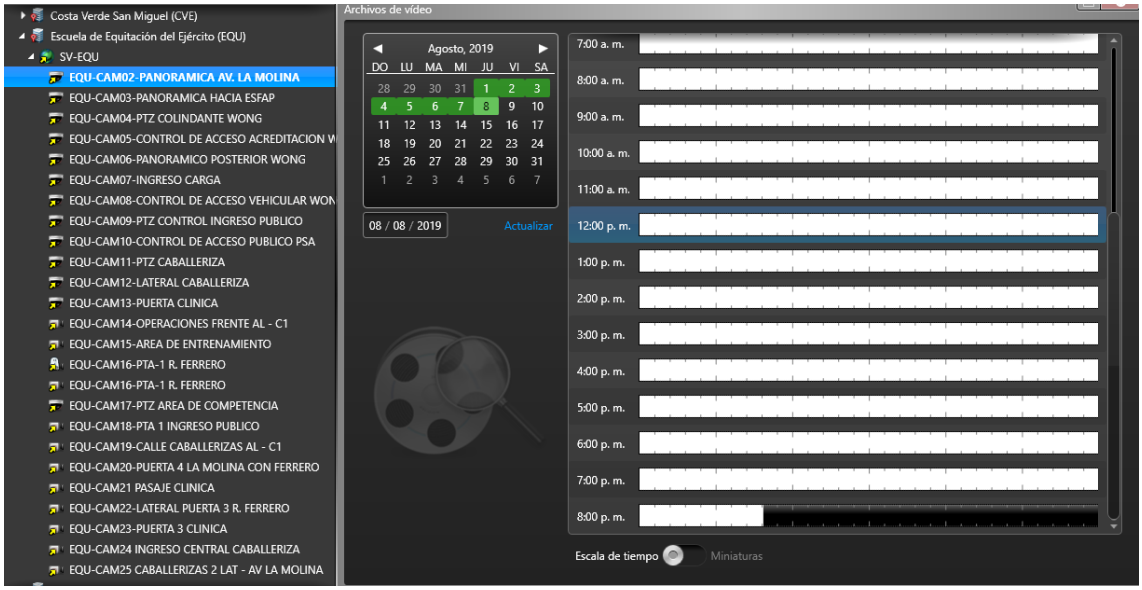


Figura 46. Sede – EQU (Escuela de Equitación del Ejército).

Fuente: Autoría propia.

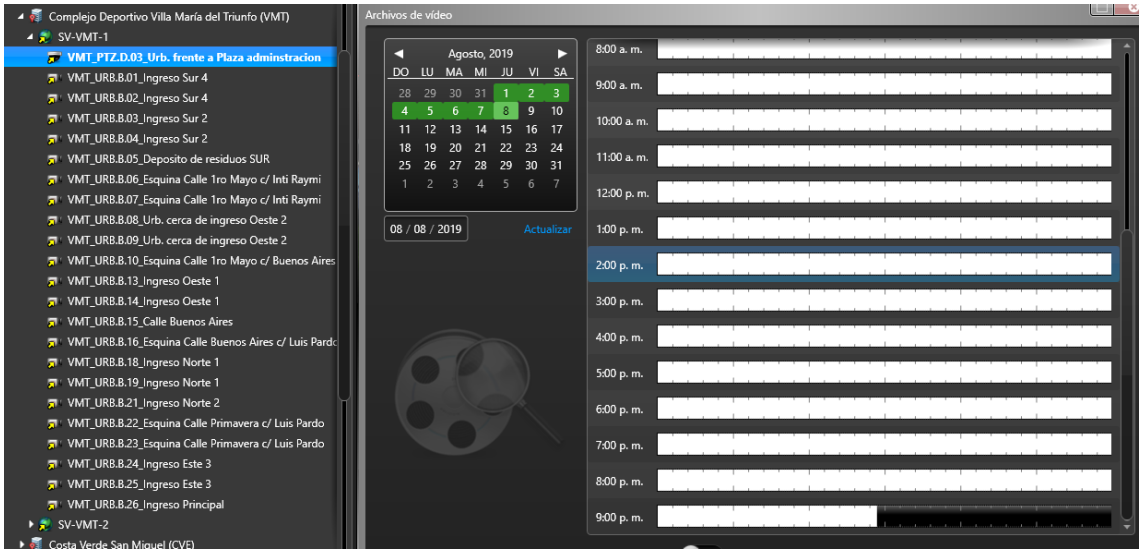


Figura 47. Sede – VMT (Complejo Deportivo Villa María del Triunfo).

Fuente: Autoría propia.

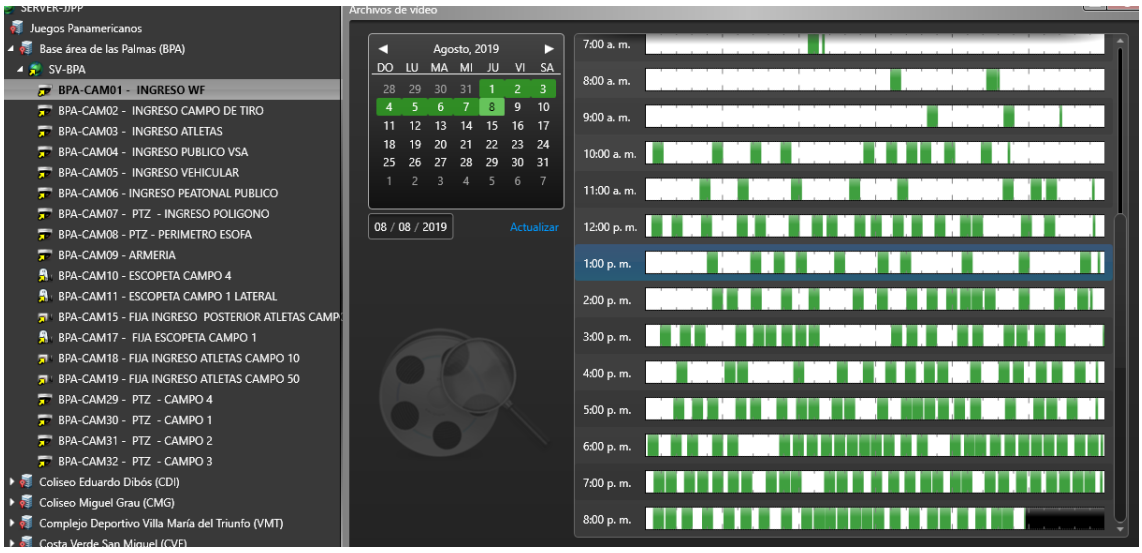


Figura 48. Sede – BPA (Base Aérea Las Palmas).

Fuente: Autoría propia.

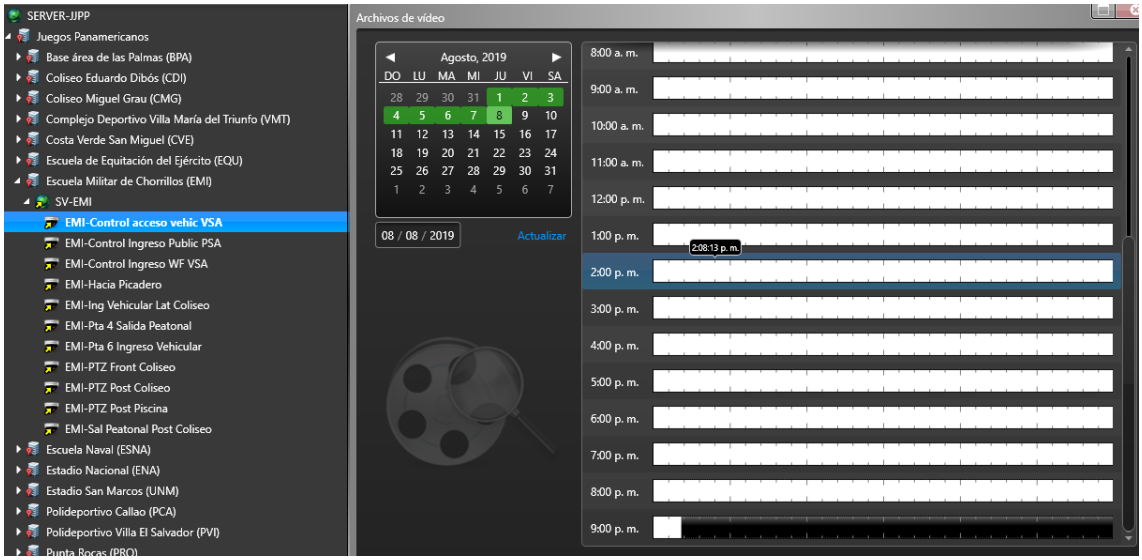


Figura 49. Sede – EMI (Escuela Militar Chorrillos).

Fuente: Autoría propia.

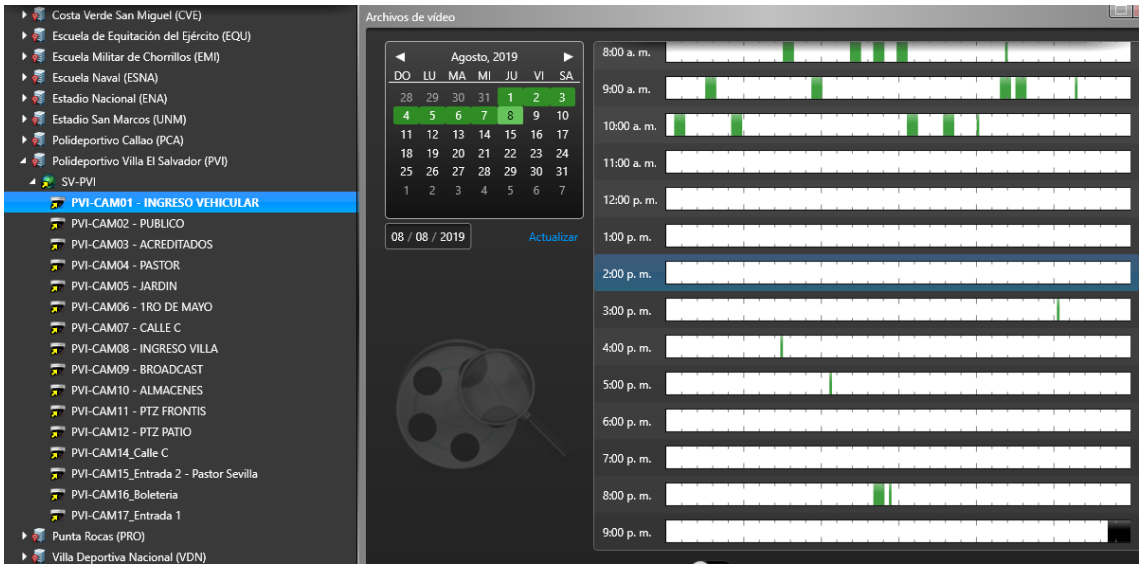


Figura 50. Sede – PVI (Polideportivo Villa El Salvador).

Fuente: Autoría propia.

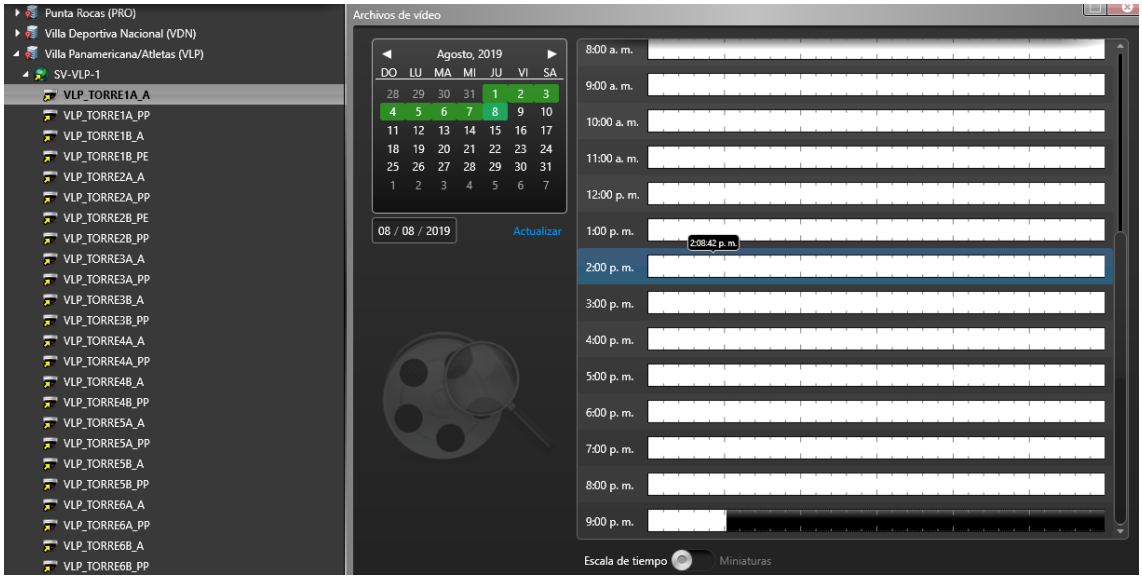


Figura 51. Sede – VLP (Villa Panamericana / Atletas).

Fuente: Autoría propia.

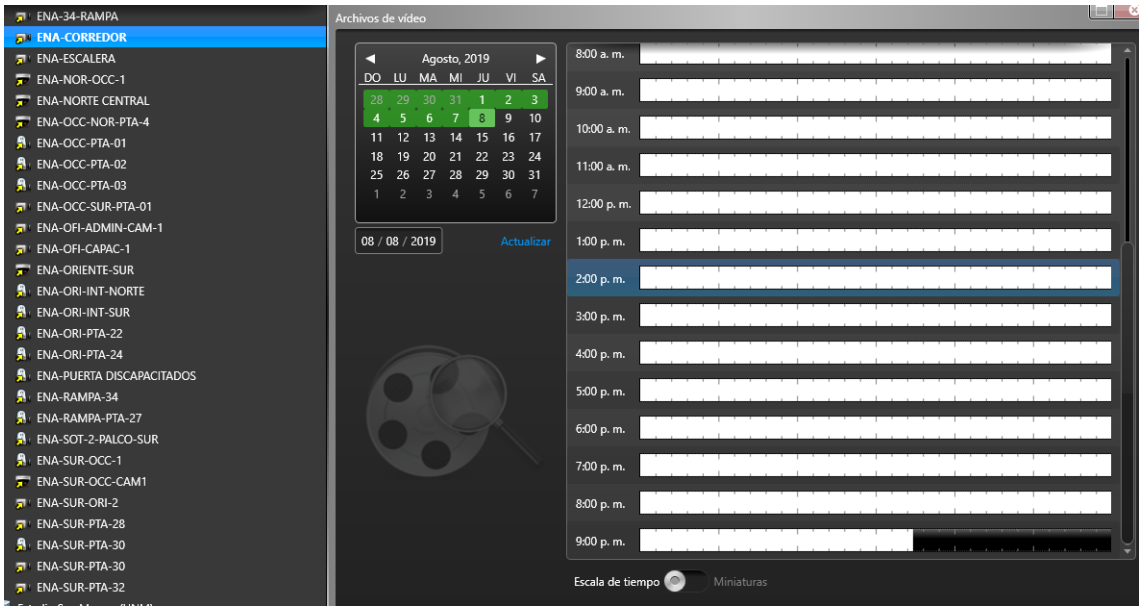


Figura 52. Sede – ENA (Estadio Nacional).

Fuente: Autoría propia.

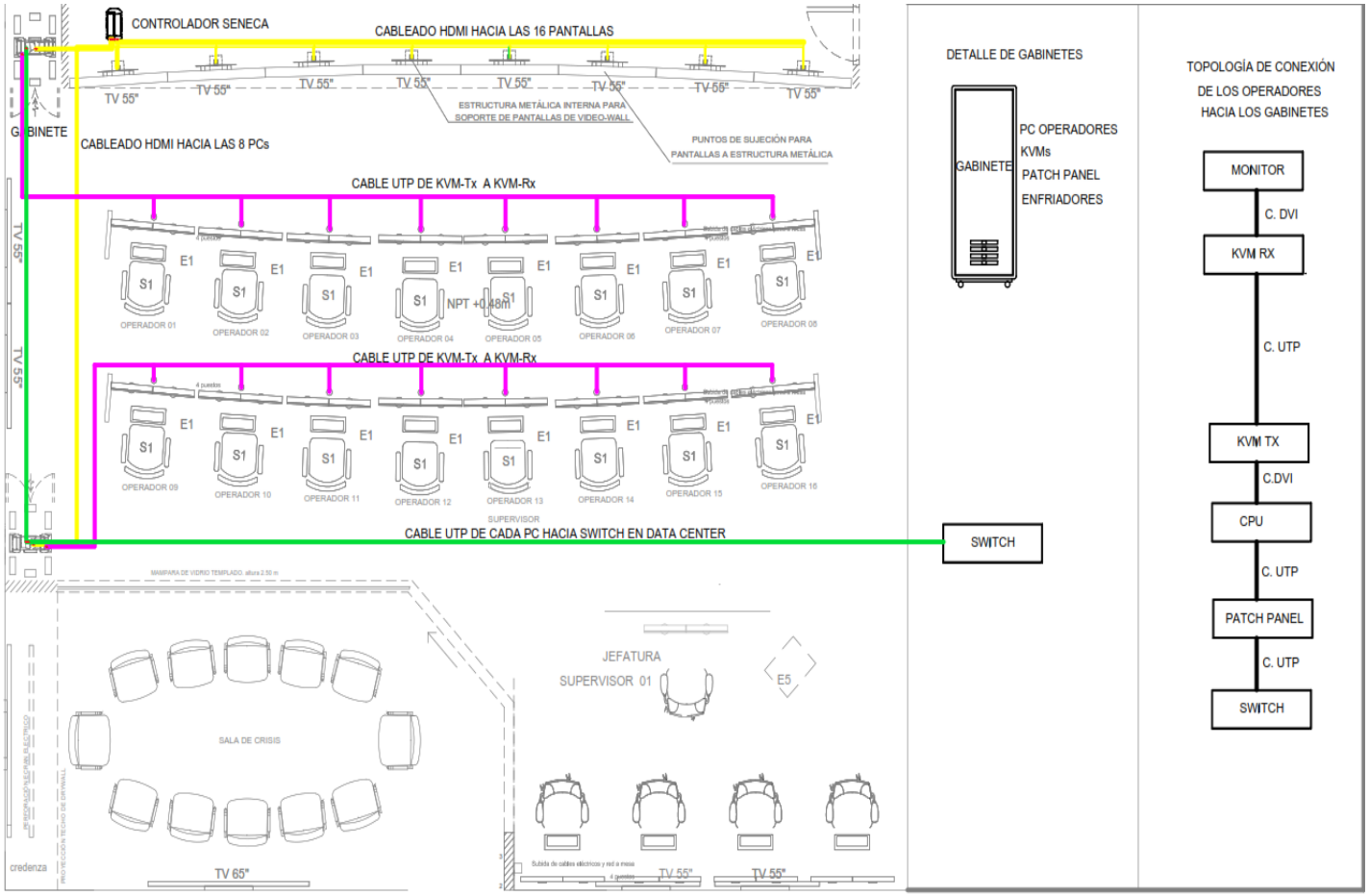


Figura 53. Plano de ubicación

Fuente: Elaboración Propia.